

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
29 December 2004 (29.12.2004)

PCT

(10) International Publication Number
WO 2004/114303 A1

(51) International Patent Classification⁷:

G11B 20/00

(21) International Application Number:

PCT/JP2004/008554

(22) International Filing Date: 11 June 2004 (11.06.2004)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2003-173908 18 June 2003 (18.06.2003) JP

(71) Applicant (for all designated States except US): MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. [JP/JP]; 1006, Oazakadoma, Kadoma-shi, Osaka 5718501 (JP).

(71) Applicant (for US only): YAMAMICHI, Masami (heir of the deceased inventor).

(72) Inventor: YAMAMICHI, Masato (deceased).

(72) Inventors; and

(75) Inventors/Applicants (for US only): YAMAMOTO, Masaya. OHMORI, Motoji. WATANABE, Kazuhisa. SASO, Atsushi. YAMAMOTO, Naoaki.

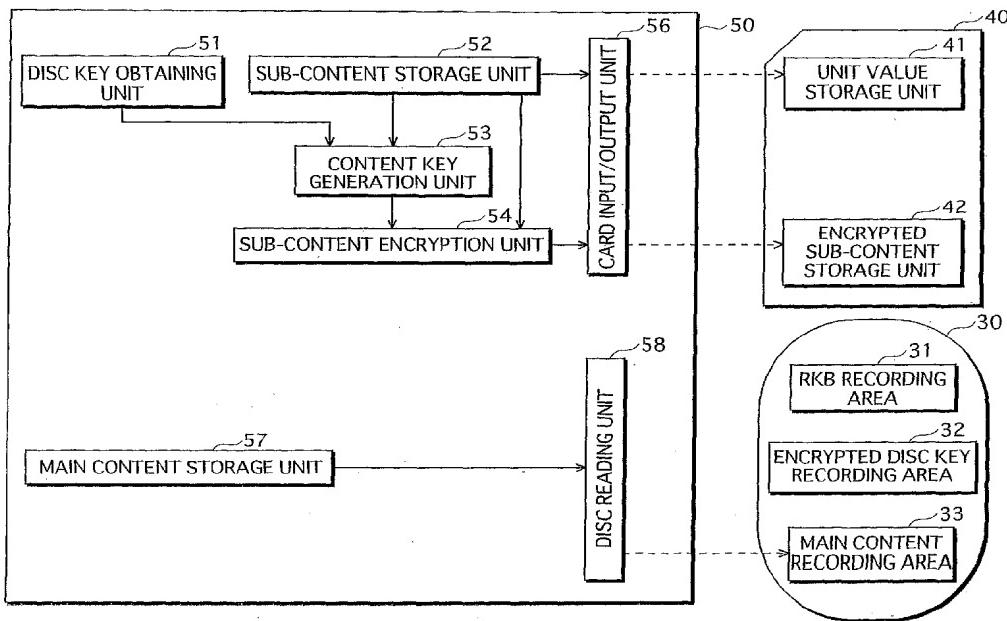
(74) Agent: NAKAJIMA, Shiro; 6F, Yodogawa 5-Bankann, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi, Osaka 5310072 (JP).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH,

/Continued on next page/

(54) Title: PLAYBACK APPARATUS, PLAYBACK METHOD, AND PROGRAM FOR REPRODUCING AN ENCRYPTED VIRTUAL PACKAGE



(57) Abstract: A content playback apparatus prevents related content recorded on separate media that make up a virtual package from being played separately, thereby restricting playback of the content to only when the virtual package is assembled as intended by the creator, and protecting copyright of the content. A key obtaining unit obtains a second key, with use of key management information recorded on a recording medium on which related content relating to the encrypted content is also recorded. An information obtaining unit obtains the encrypted content and key generation information that relates to generation of the first key, from a source other than the recording medium. A key generation unit generates the first key with use of the second key and the obtained key generation information. A decryption unit decrypts the encrypted content with use of the first key.

WO 2004/114303 A1



GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,
SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Description

PLAYBACK APPARATUS, PLAYBACK METHOD, AND PROGRAM FOR REPRODUCING
AN ENCRYPTED VIRTUAL PACKAGE

Technical Field

5 The present invention relates to a playback apparatus for playing a plurality of related contents, and in particular, to a technique for protecting copyright of the content.

Background Art

10 Digital contents have begun to be distributed in increasingly diverse forms in recent years, one of which is distribution using virtual packages.

15 A virtual package consists of a plurality of media on which mutually related digital contents are respectively recorded. The digital contents recorded on the plurality of media are treated by a playback apparatus as being recorded in one package.

20 As one example, a content creator pre-distributes large-capacity content (main content) that is a movie whose script is in English to the owner of a content playback apparatus, using a BD-ROM. After the English script has been translated into Japanese, the content creator distributes small-capacity content (sub-content) that is Japanese subtitles of the movie, using an SD card. When the sub-content has been distributed, the owner of the playback apparatus is able to watch the movie that is the main content and the Japanese subtitles that are the sub-content as if they were one content recorded in one package.

25 Since digital content is easily copied without deterioration of the information, protection of copyrights of digital content is

crucial, regardless of whether or not it is distributed as a virtual package. For this reason, in addition to recording digital content in an encrypted state on a recording medium, information that prevents the content from being decrypted with a playback apparatus key that 5 has been exposed is written to the recording medium. This technique, which is disclosed in Document 1, improves copyright protection by preventing the content being decrypted with the exposed key from recording media distributed after the key has been exposed.

However, this copyright protection is structured such that 10 decryption of encrypted content can be complete only in information in a package in which digital content is recorded. Consequently, such copyright protection is problematic in that part of the content of a virtual package can be played without having all the elements that make up the virtual package.

15 For example, sub-content on an SD card can be played with only the SD card, in other words, without the BD-ROM that is also an element of the virtual package. This is contravenes the intention of the copyright owner who created the package.

In view of the stated problem, the object of the present invention 20 is to provide a content playback apparatus that plays content recorded in a virtual package in a manner that assembles the components of the virtual package as intended by the creator, and protects the copyright thereof.

Document 1: JP, 2002-281013, A

25

Disclosure of the Invention

In order to achieve the stated object, the content playback apparatus of the present invention is a content playback apparatus

for obtaining encrypted content that has been generated by encrypting content with use of a first key, decrypting the obtained encrypted content, and playing the decrypted content, the content being encrypted based on the first key, the first key being generated by

5 applying a predetermined operation to key generation information based on a second key, the second key being recorded on a recording medium so as to be extractable from the recording medium according to a predetermined procedure, the content playback apparatus including: a key obtaining unit operable to extract the second key

10 from the recording medium according to the predetermined procedure; an information obtaining unit operable to obtain the encrypted content and the key generation information from an information source other than the recording medium; a key generation unit operable to apply the predetermined operation to the obtained key generation information,

15 based on the second key, thereby generating a third key; and a decryption unit operable to decrypt the encrypted content based on the generated third key.

According to the stated structure, by restricting decryption of encrypted content to being possible only when the second key has

20 been obtained using the information recorded on the recording medium, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the recording medium may have recorded thereon

25 key management information that is generated by encrypting the second key based on a fourth key, and the key obtaining unit may include: a key storage sub-unit operable to store the fourth key which has been pre-assigned to the content playback apparatus; an information

reading sub-unit operable to read the key management information from the recording medium; and a key obtaining sub-unit operable to obtain the second key by decrypting the key management information with use of the fourth key.

5 Playback of the content can be restricted to only a content playback apparatus that has the fourth key.

Furthermore, the recording medium may have recorded thereon key management information that is a list of encrypted second keys that have been generated by encrypting the second key respectively 10 with use of a plurality of keys equivalent to the fourth key, and the key obtaining unit may include: a key storage sub-unit operable to store the fourth key that has been pre-assigned to the content playback apparatus; an information obtaining sub-unit operable to obtain the key management information from the recording medium; 15 and a key obtaining sub-unit operable to obtain the second key by decrypting, based on the fourth key, from among the encrypted second keys of the key management information, the encrypted second key that has been encrypted based on the fourth key.

According to the stated structure, the content cannot be played 20 when the second key encrypted with the fourth key is not included in the list. Therefore, a content playback apparatus whose pre-stored key has been exposed is prevented from playing the content, and copyright of the content is protected.

Furthermore, the recording medium may have recorded thereon 25 key management information that is a list of encrypted second keys that have been generated by encrypting the second key respectively with use of valid keys, and the key obtaining unit may include: a key storage sub-unit operable to store a plurality of keys; an

information obtaining sub-unit operable to obtain the key management information from the recording medium; and a key obtaining sub-unit operable to, when one of the plurality of keys stored in the key-storage sub-unit matches one of the valid keys, decrypt, from among the 5 encrypted second keys of the key management information, an encrypted second key that has been encrypted based on the matching key, thereby obtaining the second key.

According to the structure, the content cannot be played if none of the encrypted second keys encrypted with the plurality of 10 keys stored by the content playback apparatus is included in the list. Therefore, permission for the playback apparatus to play the content can be controlled by modifying the contents of the list, and copyright of the content is protected.

Furthermore, the recording medium have recorded thereon key 15 management information including a list of encrypted fifth keys that have been generated by encrypting a fifth key respectively with a plurality of keys, and an encrypted second key that has been generated by encrypting the second key with the fifth key, and the key obtaining unit may include: a key storage sub-unit operable to store a fourth 20 key that has been pre-assigned to the content playback apparatus; an information obtaining sub-unit operable to obtain the key management information from the recording medium; a first key obtaining sub-unit operable to decrypt the encrypted fifth keys of the key management information respectively with use of the fourth 25 key; and a second key obtaining sub-unit operable to, when the decryption by the first key obtaining sub-unit succeeds, decrypt the encrypted second key with the fifth key resulting from the decryption by the first key obtaining sub-unit, thereby obtaining

the second key.

According to the stated structure, by restricting decryption of the encrypted content to cases in which the fifth key and the second key have been obtained using the fourth key, the content can be 5 restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the key generation information may be an encrypted first key that has been generated by encrypting the first key with use of the second key, and the key generation unit may generate the 10 third key by decrypting the obtained key generation information with the second key.

According to the stated structure, by restricting the decryption of content to when the third key having the same value as the first key has been obtained by decrypting the key generation 15 information with the second key, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the key generation information may be arbitrary data of a predetermined length, and may be in correspondence with 20 the content, and the first key may have been obtained as a result of subjecting the key generation information to one-way function processing according to a predetermined encryption method, based on the second key, and the key generation unit may subject the key generation information to one-way function processing based on a 25 predetermined encryption method, based on the second key, and treat resultant data as the third key.

According to the stated structure, by restricting decryption of encrypted content, which has been encrypted based on a predetermined

encryption method and using one-way function processing, to when the third key having the same value as the first key has been generated using the key generation information, the content can be restricted to being played only when the virtual package is assembled as intended
5 by the creator, and copyright can be protected.

Furthermore, the first key may be an exclusive OR of the key generation information and encrypted key generation information generated by encrypting the key generation information based on the predetermined encryption method, with use of the second key, and
10 the key generation unit may include: an encryption sub-unit operable to encrypt the key generation information based on the predetermined encryption method, with use of the second key; and a calculation sub-unit operable to calculate an exclusive OR of the key generation information and the encrypted key generation information, and treat
15 the resultant data as the third key.

According to the stated structure, by restricting decryption of encrypted content, which has been encrypted based on a predetermined encryption method and using one-way function processing, to when the third key having the same value as the first key has been obtained
20 using the key generation information, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.
25

Furthermore, the predetermined encryption method may be an AES encryption method, and the encryption unit may encrypt the key generation information according to the AES encryption method, based on the second key.

According to the stated structure, by restricting decryption of encrypted content, which has been encrypted based on a predetermined

encryption method and using one-way function processing, to when the third key having the same value as the first key has been obtained using the key generation information, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the information obtaining unit may obtain the encrypted content and the key generation information via a network.

According to the stated structure, by restricting decryption of the encrypted content to when the second key is obtained using information recorded on the recording medium, playback of the content can be restricted a manner that assembles the components of the virtual package consisting of the recording medium and a content provider connected to via a network, as intended by the creator, and copyright can be protected.

Furthermore, the information obtaining unit may obtain the encrypted content and the key generation information from a dependant recording medium that is separate from the recording medium.

According to the stated structure, by restricting decryption of the encrypted content to when the third key having the same value as the first key is obtained using the key generation information, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the recording medium may have recorded thereon key management information that includes a list of encrypted fifth keys that have been generated by encrypting a fifth key respectively with each of a plurality of keys, and encrypted key generation information that has been generated by encrypting the key information

with the fifth key, the information obtaining unit may include: a key storage sub-unit operable to store a fourth key that has been pre-assigned to the content playback apparatus; an information reading sub-unit operable to read the encrypted content and the key management information from the defendant recording medium; a first key obtaining sub-unit operable to decrypt the encrypted fifth keys of the key management information, based on the fourth key; and a second key obtaining sub-unit operable to, when the decryption by the first key obtaining sub-unit succeeds, decrypt the encrypted key generation information with use of the fifth key generated as a result of the decryption by the first key obtaining sub-unit.

According to the stated structure, by restricting decryption of the encrypted content to when the fifth key and the second key are obtained using the fourth key, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the information obtaining unit may obtain the encrypted content and the key generation information from a memory card separate from the recording medium.

According to the stated structure, by restricting decryption of the encrypted content to when the third key having the same value as the first key is obtained using the key generation information, playback of the content can be restricted a manner that assembles the components of the virtual package consisting of the recording medium and a memory card that is separate to the recording medium, as intended by the creator, and copyright can be protected.

Furthermore, the information obtaining unit may obtain the encrypted content and the key generation information from a disc

separate from the recording medium.

According to the stated structure, by restricting decryption of the encrypted content to when the third key having the same value as the first key is obtained using the key generation information, 5 playback of the content can be restricted a manner that assembles the components of the virtual package consisting of the recording medium and a disc that is separate to the recording medium, as intended by the creator, and copyright can be protected.

Furthermore, the encrypted content may have been generated 10 by encrypting the content with use of a block encryption method, based on the first key, and the decryption unit may decrypt the encrypted content with use of the block encryption method, based on the first key.

According to the stated structure, by restricting decryption 15 of the encrypted content, that has been encrypted based on a block encryption method, to when the third key having the same value as the first key is obtained, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

20 Furthermore, the encrypted content may have been generated by encrypting the content with use of a C2 encryption method, based on the first key, and the decryption unit may decrypt the encrypted content with use of the C2 encryption method, based on the first key.

25 According to the stated structure, by restricting decryption of the encrypted content, that has been encrypted based on a C2 encryption method, to when the third key having the same value as the first key is obtained, the content can be restricted to being

played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the encrypted content may have been generated by encrypting the content with use of a DES encryption method, based on the first key, and the decryption unit may decrypt the encrypted content with use of the DES encryption method, based on the first key.

According to the stated structure, by restricting decryption of the encrypted content, that has been encrypted based on a DES encryption method, to when the third key having the same value as the first key is obtained, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Furthermore, the encrypted content may have been generated by encrypting the content with use of an AES encryption method, based on the first key, and the decryption unit may decrypt the encrypted content with use of the AES encryption method, based on the first key.

According to the stated structure, by restricting decryption of the encrypted content, that has been encrypted based on an AES encryption method, to when the third key having the same value as the first key is obtained, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

The content playback method of the present invention is a content playback method used in a content playback apparatus that includes a key obtaining unit, an information obtaining unit, a key generation unit and a decryption unit, and is for obtaining encrypted content

that has been generated by encrypting content with a first key, and playing the decrypted content, the content being encrypted based on the first key, the first key being generated by applying a predetermined operation to key generation information based on a second key, the second key being recorded on a recording medium so as to be extractable from the recording medium according to a predetermined procedure, the content playback method including: a key obtaining step of extracting the second key from the recording medium according to the predetermined procedure; an information obtaining step of obtaining the encrypted content and the key generation information from an information source other than the recording medium; a key generation step of applying the predetermined operation to the obtained key generation information, based on the second key, thereby generating a third key; and a decryption step of decrypting the encrypted content based on the generated third key.

According to the stated structure, by restricting decryption of the encrypted content to when the second key is obtained using the information recorded on the recording medium, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

The program of the present invention is a program applied to a content playback apparatus that includes a key obtaining unit, an information obtaining unit, a key generation unit and a decryption unit, and is for obtaining encrypted content that has been generated by encrypting content with a first key, and playing the decrypted content, the content being encrypted based on the first key, the first key being generated by applying a predetermined operation to

key generation information based on a second key, the second key being recorded on a recording medium so as to be extractable from the recording medium according to a predetermined procedure, the program having a computer execute: a key obtaining step of extracting 5 the second key from the recording medium according to the predetermined procedure; an information obtaining step of obtaining the encrypted content and the key generation information from an information source other than the recording medium; a key generation step of applying the predetermined operation to the obtained key generation information, 10 based on the second key, thereby generating a third key; and a decryption step of decrypting the encrypted content based on the generated third key.

According to the stated structure, by restricting decryption of the encrypted content to when the second key is obtained using 15 the information recorded on the recording medium, the content can be restricted to being played only when the virtual package is assembled as intended by the creator, and copyright can be protected.

Brief Description of the Drawings

20 FIG. 1 shows an outline of a content playback system of the present invention;

FIG. 2 is a block diagram of the structure of a key management apparatus;

FIG. 3 shows schematically information written on a BD-ROM;

25 FIG. 4 is a block diagram showing the structure of a recording apparatus;

FIG. 5 shows an example of data stored in a sub-content storage unit;

FIG. 6 shows schematically data stored in a unit value holding unit and an encrypted sub-content storage unit of an SD card;

FIG. 7 is a block diagram showing the structure of a playback apparatus;

5 FIG. 8 is a flowchart showing operations by the playback apparatus when playing content;

FIG. 9 is a schematic drawing of a content playback system of a second embodiment of the present invention;

10 FIG. 10 shows information relating to content stored by an SD card;

FIG. 11 is a block diagram showing the structure of the content playback system in terms of function;

FIG. 12 shows information relating to playback control, held by a control unit;

15 FIG. 13 is a flowchart showing content playback processing in the content playback system;

FIG. 14 is a schematic drawing of the content playback system of a third embodiment of the present invention;

20 FIG. 15 is a block diagram showing the structure of the content playback system of the third embodiment;

FIG. 16 shows a content playback control table; and

FIG. 17 is a flowchart showing content playback processing in the content playback system.

25 Best Mode for Carrying Out the Invention

<First Embodiment>

The following describes a content playback system of the first embodiment with use of the drawings.

First, an overview of the content playback system is given.

The object of the content playback system is, in the case of a virtual package that consists of (1) packaged media on which is recorded main content that is audio and video data or the like, and
5 (2) package media on which is recorded sub-content that is data such as subtitles relating to the main content, to restrict decryption and playback of the sub-content such that it is able to be played only when a user also owns the main content packaged media, in other words, when the user has rights to the sub-content, and improve
10 protection of copyright.

Specifically, here an example is used of the main content being a data stream, or the like, relating to audio and video of a movie, and the sub-content being a data stream of Japanese or Korean subtitles, or the like, that is not included in the main content. Furthermore,
15 the copyright owner has created the sub-content with the intention that it be viewed only by a user who has purchased a packaged media on which the main content is recorded. The sub-content is not limited to being distributed as packaged media, but may be distributed over a communication wire, through broadcasting, or in another manner.

20 FIG. 1 is an outline of the content playback system.

The content playback system is composed of a plurality of playback apparatuses 10a, 10b, 10c, 10d, 10e, etc., a BD-ROM 30, an SD card 40, a key management apparatus 70, and a recording apparatus 50. The playback apparatuses 10a, 10b, 10c, 10d, 10e, etc. are for
25 playing the main content and the sub-content. The main content and related information are recorded on the BD-ROM 30. The sub-content and related information are recorded on the SD card 40, the sub-content being in an encrypted state. The key management apparatus 70 manages

keys such as device keys that are assigned and distributed to the playback apparatuses, the device key of each playback apparatus being unique to that playback apparatus. In addition, the key management apparatus 70 writes various key information to a lead-in area or 5 the like of the BD-ROM 30 during the BD-ROM manufacturing process. The recording apparatus 50 records information including content to the BD-ROM 30 and the SD card 40.

Note that in the following, content is played by a playback apparatus 10 which is one of the playback apparatuses 10a, 10b, 10c, 10d, 10e, etc.

The key management system 70 writes key management information and other information to the lead-in area or the like of the BD-ROM 30, and then transfers the BD-ROM 30 to the recording apparatus 50.

The key management information is for revoking a predetermined device 15 key or keys among the device keys distributed to the playback apparatuses.

The recording apparatus 50 is a content recording apparatus that includes a content editing function and is a personal computer or the like to which a keyboard 51 for operations, a monitor 52, 20 and so on, are connected. The recording apparatus 50 writes main content to the BD-ROM 30 and sub-content relating to the main content to the SD card 40.

The BD-ROM 30 and the SD card 40 to which information has been written by the recording apparatus 50 are transferred to the user 25 of the playback apparatus 10 through a retail shop. The user of the playback apparatus 10 inserts the obtained BD-ROM 30 and SD card 40 in respective insertion slots in the playback apparatus 10.

The playback apparatus 10 is a drive apparatus for reading

the content of the BD-ROM 30, and is, specifically, a BD player or the like that includes a card reader/writer for reading and writing data from and to the SD card 40, and an optical unit for receiving instructions from a remote control 20. In accordance with an instruction given by the user using the remote control 20, the playback apparatus 10 plays content recorded on the BD-ROM 30 and the SD card 40, and outputs the played content to a monitor 21 which displays the content.

The following describes the key management apparatus 70.

FIG. 2 is a block diagram showing the structure of the key management apparatus 70.

The key management apparatus 70, as shown in FIG. 2, is composed of a device key storage unit 71, a media key storage unit 72, an RKB generation unit 73, a disc key storage unit 74, an encrypted disc key generation unit 75, and a disc input/output unit 76. Specifically, the key management apparatus 70 is a computer system that includes a CPU, a ROM, a RAM, a hard disc, and a disc drive or a disc machining apparatus that machines discs. A computer program is stored in the ROM, and the computer system achieves its functions by the CPU operating according to the computer program.

The device key storage unit 71 pre-stores valid device keys among the device keys distributed to the playback devices.

Each device key is data of a fixed bit-length (256 bytes, for example) that is pre-assigned uniquely to one of the playback apparatuses.

The key storage unit 72 pre-stores media keys, each of which is assigned to each of a predetermined number of recording media (per dispatch lot, for example).

The media keys are notified by the recording medium manufacturer in advance. Here, the media key of the BD-ROM 30 is called Km.

The RKB (renewal key block) generation unit 73 is a list of encrypted media keys obtained as a result of encrypting Km with each 5 of the device keys stored in the device key storage unit 71.

FIG. 3 shows an overview of information written in the BD-ROM 30.

As shown in FIG. 3, apparatus numbers assigned uniquely to the playback apparatuses and an encrypted media key are stored in 10 correspondence as an RKB in an RKB recording area 31.

Kdev_1 represents a device key assigned to a playback apparatus whose device number is "1". E1(Kdev_1, Km) represents Km encrypted with Kdev_1 according to an encryption method E1.

Furthermore, E1(Kdev_2, 0) is recorded in correspondence with 15 a playback apparatus "2". The result of decrypting E1(Kdev_2, 0) with a device key Kdev_2 will be "0", not a media key. This indicates that the apparatus of apparatus number 2 is revoked.

A commonly known method such as AES (advanced encryption standard) is suitable for the encryption method E1.

20 The RKB generation unit 73 records an RKB (described later) in the RKB recording area of the BD-ROM 30 via the disc input/output unit 76.

The disc key storage unit 74 stores disc keys, each of which 25 is a key unique to one BD-ROM. The number of disc keys stored is equal to the number of BD-ROMs.

The disc key corresponding to the BD-ROM 30 is called Kd here.

The encrypted disc key generation unit 75 obtains Km from the media key storage unit 72, obtains Kd from the disc key storage unit

74, and encrypts Kd with Km using the AES encryption method.

Details of the AES encryption method can be found on the NIST (National Institute of Standards and Technology) website (<http://csrc.nist.gov/CryptoToolkit/aes/>), and are therefore omitted from the present description.

Hereinafter, Em(Kd) expresses Kd that has been encrypted using Km.

The encrypted disc key generation unit 75 records the generated Em(Kd) as shown in FIG. 3 to an encrypted disc key recording area 10 32 of the BD-ROM 30 via the disc input/output unit 76.

The disc key transmission unit 77 notifies the recording apparatus 50 of the disc key used in the encrypted disc key generation unit 75, via a network.

The following describes the recording apparatus 50.

15 FIG. 4 is a block diagram showing the structure of the recording apparatus 50.

As shown in FIG. 4, the recording apparatus 50 is composed of a disc key obtaining unit 51, a sub-content storage unit 52, a content key generation unit 53, a sub-content encryption unit 54, 20 a card input/output unit 56, a main content storage unit 57, and a disc write unit 58. Specifically, the recording apparatus 50 is a computer system that includes a CPU, a ROM, a RAM, a hard disc, a memory card reader/writer, and a disc drive or a disc machining apparatus that machines discs. A computer program is stored in the 25 ROM, and the computer system achieves its functions by the CPU operating according to the computer program.

The disc key obtaining unit 51 obtains a disc key from the key management apparatus 70 via a network, and outputs the obtained

disc key to the content key generation unit 53.

Here, the disc transferred from the key management apparatus 70 is the BD-ROM 30, and the disc key obtained by the disc key obtaining unit 51 is Kd.

5 The sub-content storage unit 52 pre-stores content numbers that identify sub-content, unit values, each of which is a value of a predetermined length (128 bits, for example) unique to a sub-content, and sub-contents, in correspondence.

FIG. 5 shows an example of data stored in the sub-content storage
10 unit 52. For example, sub-content 1 is stored in correspondence with a content number "1", and a unit value having a value "Vu_1".

The sub-content storage unit 52 outputs a unit value corresponding to sub-content to be encrypted to the content key generation unit 53 and the card input/output unit 56, and outputs
15 the sub-content corresponding to the output unit value to the sub-content encryption unit 54.

The content key generation unit 53 applies a one-way function, which utilizes an AES encryption, to the unit value obtained from the sub-content storage unit 52, outputs an exclusive OR of the result
20 of applying the one-way function and the unit value to the sub-content encryption unit 54 as a content key Ku.

The content encryption unit 54 obtains the sub-content from the sub-content storage unit 52, and encrypts the obtained sub-content with the content key Ku.

25 A commonly known method such as AES is suitable for the encryption method.

The card input/output unit 56 writes the received unit value to the unit value storage unit 41 of the SD card 40, and records

the encrypted sub-content to the encrypted sub-content storage unit 42 of the SD card 40.

FIG. 6 shows data stored in the unit value storage unit 41 and the encrypted sub-content storage unit 42 of the SD card 40, 5 schematically. Each piece of data recorded in the unit value storage unit 41 is in correspondence with a piece of data recorded in the same position in the order in the encrypted sub-content storage unit 42.

For example, Vu_1 and E2(Ku_1, sub-content 1) are in 10 correspondence, and Vu_m and E2(Ku_m, sub-content m) are in correspondence.

The main content storage unit 57 stores main content, and outputs the main content to the disc writing unit 58 which writes the main content to the main content recording area 33 of the BD-ROM 30, as 15 shown in FIG. 3.

The following describes the playback apparatus 10.

In this example, the playback apparatus 10 is the playback apparatus having the apparatus number "1" in FIG. 3.

FIG. 7 is a block diagram showing the structure of the playback 20 apparatus 10.

The playback apparatus 10, as shown in FIG. 7, is composed of an instruction obtaining unit 11, a control unit 12, a disc input/output unit 13, a device key storage unit 14, an RKB processing unit 15, a disc key generation unit 16, a card input/output unit 25 17, a content key generation unit 18, a sub-content decryption unit 19, and a playback unit 20. Specifically, the playback apparatus 10 is a BD player or the like that includes a CPU, a ROM, a RAM, an MPEG (moving picture experts group) decoder, an audio/video signal

processing unit, an encryption processing unit, a disc drive, and a card reader/writer. A computer program is stored in the ROM, and the BD player achieves its functions by the CPU operating according to the computer program.

5 The instruction obtaining unit 11 obtains a user instruction corresponding to a user operation of the remote control 20, from the remote control 20, and transmits the obtained instruction to the control unit 12.

10 One type of user instruction is a content playback instruction that includes a content ID identifying content that the user desires to have played.

15 Specifically, the control unit 12 is the CPU and the computer program, and controls overall operations of the playback apparatus 10.

20 On receiving the content playback instruction, the control unit 12 instructs the disc input/output unit 13 to read an RKB from the BD-ROM 30, instructs the RKB processing unit 15 to process the RKB, instructs the card input/output unit 17 to read the unit value and the encrypted sub-content, and instructs the playback unit 20 to play the sub-content.

25 The disc input/output unit 13 includes a disc drive for reading information from the BD-ROM and the control unit of the disc drive. The disc input/output unit 13 reads the RKB from the BD-ROM in accordance with the instruction from the control unit 12 and outputs the read RKB to the RKB processing unit 15, reads Em(Kd) from the BD-ROM 30 and outputs the read Em(Kd) to the disc key generation unit 16, and reads the main content from the BD-ROM 30 and outputs the read main content to the playback unit 20.

The device key storage unit 14 is a non-volatile memory, and pre-stores a device key Kdev_1 that is a key unique to the playback apparatus.

The RKB processing unit 15, in accordance with the instruction 5 from the control unit 12, after reading the device key Kdev_1 from the device key storage unit 14 and reading the RKB from the RKB storage area 31 of the BD-ROM 30 via the disc input/output unit 13, decrypts the encrypted media key E1(Kdev_1, Km), which corresponds to apparatus number "1" in the RKB in FIG. 3, with the device key Kdev_1 based 10 on the AES encryption method, thereby obtaining Km. The RKB processing unit 15 then outputs the generated Km to the disc key generation unit 16.

Here, if, for example, the playback apparatus 10 is the apparatus having the revoked apparatus number "2", a value "0" will be obtained 15 in the decryption processing in the RKB processing unit 15, and generation of the media key Km will fail. Consequently, decryption of the sub-content will fail.

The disc key generation unit 16 is an encryption processing unit that decrypts information in accordance with the AES encryption 20 method. The disc key generation unit 16 obtains Km from the RKB processing unit 15, obtains Em(Kd) via the disc input/output unit 13, and decrypts Em(Kd) using Km based on the AES encryption method, thereby obtaining a disc key Kd.

The card input/output unit 17 is a card reader/writer that 25 transfers information to and from the SD card 40. The card input/output unit 17 outputs the unit value read from the unit value storage unit 41 of the SD card 40 to the content key generation unit 18, and outputs encrypted sub-content read from the encrypted

sub-content storage unit 42 to the sub-content decryption unit 19.

The content key generation unit 18 is an encryption processing unit that performs one-way function processing in accordance with the AES encryption. The content key generation unit 18 obtains the 5 unit value from the unit value storage unit 41 of the SD card 40 via the card input/output unit 17, and obtains Kd from the disc key generation unit 16. The content key generation unit 18 then applies one-way function processing to the unit value with Kd in accordance with the AES encryption method, and outputs an exclusive OR of the 10 result of the one-way function and the unit value to the sub-content decryption unit 19 as a content key Ku.

The sub-content decryption unit 19 obtains the encrypted sub-content from the encrypted sub-content storage unit 42 via the card input/output unit 17, and decrypts the encrypted sub-content 15 using the content key Ku based on a predetermined encryption method (AES, for example).

The playback unit 20 is composed of an MPEG decoder and an audio/video signal processing unit. The playback unit 20 generates audio and video signals from the main content and the sub-content, 20 and outputs the signals to the monitor 21.

The following describes operations of the playback apparatus 10 for decrypting and playing sub-content.

In the present example, it is assumed the playback apparatus 10 has the apparatus number "1", and has been instructed by the user 25 to play "sub-content 1" that has a content number "1".

FIG. 8 is a flowchart showing operations when the playback apparatus 10 plays content.

The user of the playback apparatus 10 inserts the BD-ROM 30

in the disc drive of the playback apparatus 10, and inserts the SD card 40 in the card reader/writer of the playback apparatus 10.

The user uses the remote control 20 to instruct the playback apparatus to play the sub-content 1 that has the content number "1" 5 (step S1).

The instruction obtaining unit 11 obtains a user instruction instructing playback of the sub-content 1, from the remote control 20, and transmits the received user instruction to the control unit 12.

10 The control unit 12 obtains the user instruction, stores the value "1" as the content number of the content to be played, and instructs the RKB processing unit 15 to read the RKB.

The RKB processing unit 15 reads the RKB from the RKB recording area 31 of the BD-ROM 30 via the disc input/output unit 13 (step 15 S2).

The RKB processing unit 15 obtains the device key K_{dev_1} from the device key storage unit 14, extracts $E1(K_{dev_1}, Km)$, which corresponds to the apparatus "1", from the RKB, and decrypts $E1(K_{dev_1}, Km)$ with K_{dev_1} (step S3).

20 When Km fails to be obtained according to the decryption at step S3 (step S4: NO), the processing ends.

When Km is successfully obtained according to the decryption at step S3 (step S4: YES), the disc key generation unit 16 reads $Em(Kd)$ from the encrypted disc key storage area 32 of the BD-ROM 25 30 via the disc input/output unit 13 (step S5).

The disc key generation unit 16 decrypts $Em(Kd)$ with Km , thereby obtaining Kd , and outputs Kd to the content key generation unit 18 (step S6).

The content key generation unit 18 reads Vu_1, which is the unit value corresponding to the content number "1" stored by the control unit 12, from the unit value storage unit 41 of the SD card 40, via the card input/output unit 17 (step S7).

5 The content key generation unit 18 applies one-way function processing with Kd to Vu_1 in accordance with the AES encryption method, and outputs an exclusive OR of the result of the one-way function processing and Vu_1 to the sub-content decryption unit 19 as a content key Ku_1 (step S8).

10 The sub-content decryption unit 19 obtains Ku_1, and reads "encrypted sub-content 1", which corresponds to the content number "1" stored by the control unit 12, from the encrypted sub-content storage unit 42 via the card input/output unit 17 (step S9).

15 The sub-content decryption unit 19 decrypts the encrypted sub-content 1 using the content key Ku_1, and outputs the decrypted sub-content 1 to the playback unit 20 (step S10).

20 The playback unit 20 reads the main content form the main content storage unit 33 via the disc input/output unit 13, and obtains the sub-content from the sub-content decryption unit 19. The playback unit 20 then generates audio and video signals from the main content and the sub-content, and outputs the audio and video signals to the monitor 21 (step S11).

25 As has been described, according to the content playback system of the present invention, playback of sub-content by the playback apparatus is restricted to cases in which the packaged media on which content is recorded is inserted in the disc drive of the playback apparatus and the disc key Kd is able to be obtained.

Furthermore, the unit value may be distributed together with

the encrypted sub-content, thus eliminating the need to generate a unit value in advance when creating the main content.

Furthermore, the present invention makes encrypting of each sub-content using different content keys simpler, and even if a unit 5 value is exposed, effects of the exposition can be kept local, so as to only effect the sub-content corresponding to the exposed unit value.

<Modifications of the first embodiment>

(1) Although AES is described as being used for encrypting 10 and decrypting in the present embodiment, another encryption method such as DES (data encryption standard) or C2 may be used.

(2) The recording medium is not limited to having an encrypted disc key and an RKB stored thereon as in the present embodiment. For example, the disc key may be stored directly on the recording 15 medium. However, in such a case, it is necessary to record the disc key using a special method in order to prevent the disc key being read by an illegal playback apparatus. As an example of the special method, information may be cut into the BCA (Burst Cutting Area) of the disc with a special laser.

(3) The recording medium that stores the sub-content is not 20 limited to storing only the unit value and the encrypted content as described in the present embodiment. Instead, an encrypted disc key and an RKB may be stored thereon. In this case, the unit value corresponding to the sub-content is stored in an encrypted state, 25 having been encrypted with a disc key obtained from the RKB and the encrypted disc key. The playback apparatus obtains the unit value from the recording medium on which the sub-content is stored, obtains a disc key from the RKB and the encrypted disc key stored on the

sub-content recording medium, and generates a key for decrypting the content from the obtained unit value and disc key which is derived from the RKB and the encrypted disc key stored on the main content recording medium.

5

<Second Embodiment>

The following describes the second embodiment of the present invention with use of the drawings.

<Overview>

10 FIG. 9 is a schematic drawing of a content playback system 100 of the second embodiment of the present invention.

A BD (Blu-ray Disc) player 122 is a content playback apparatus that plays content stored on a BD-ROM or an SD card. The BD player 122 includes a function of performing radio communication with a 15 radio frequency tag.

A package 101 is composed of a BD-ROM 102, which is a medium on which content is stored, a box 103 in which the BD-ROM 102 is stored, and a radio frequency tag 104 that is an authentication device attached to the box 103.

20 The radio frequency tag 104 performs radio communication with the BD player 122.

The content recorded on the BD-ROM 102 is stream information that is a data stream of audio and video of a movie called "Galaxy Wars, Part 1."

25 A package 111 is composed of a BD-ROM 112, a box 113 that stores the BD-ROM 112, and a radio frequency tag 114 that is attached to the box 113.

The radio frequency tag 114 performs radio communication with

the BD player 122.

The BD-ROM 112 stores stream information of a data stream of audio and video of a movie of the title "Galaxy Wars: Part 2", which is the sequel to "Galaxy Wars: Part 1" recorded on the BD-ROM 102.

5 Here, it is assumed that a user of the BD player 122 already possesses the package 101 and the package 111.

In order to have the BD player 122 play the content stored on either the BD-ROM 102 or the BD-ROM 112, the user inserts the one of the BD-ROMs that stores the content that the user wishes to 10 play into a predetermined BD-ROM slot.

The BD player 122 reads the content that the user wishes to play from the inserted BD-ROM, and plays the read content.

Furthermore, the user transmits user instructions to the BD player 122 with use of a remote control 123 by pressing operation 15 keys such as a fast forward key, a rewind key, and a stop key.

On receiving a user instruction, the BD player 122 performs control relating to content playback, such as fast forwarding, rewinding, and stopping, in accordance with the user instruction.

20 The SD card 121 is a recording medium on which content is recorded, and is distributed to the user separately to the package 101 or the package 111.

The SD card 121 is electrically connected to the BD player 122 by being mounted in the predetermined SD card slot therein.

25 The SD memory card 121 stores stream information that is a data stream of audio and video of a program related to the movie stored on the BD-ROM, such as a behind-the-scenes video of the movie, or a commercial video or the like that is unrelated to the movie.

Here, a behind-the-scenes video is a video that, for example,

shows how the movie was filmed, secrets of the filming, or the activities of the performers in the movie during waiting time in the filming. A commercial video is a video for advertising a product or the like that is not related to the main feature movie.

5 FIGS. 10A and 10B show information relating to content stored on the SD card 121.

FIG. 10A shows content stored on the SD card 121.

The SD card 121 stores four contents: contents 151, 152, 153, and 154.

10 The content 151 is stream information of a commercial video that is unrelated to the movie.

The content 152 is encrypted information generated by encrypting data stream information of a behind-the-scenes video of the movie "Galaxy Wars: Part 1" with use of a first content key.

15 The content 152 can be decrypted with the first content key.

The content 153 is encrypted information generated by encrypting data stream information of a behind-the-scenes video of the movie "Galaxy Wars: Part 2" with use of a second content key. The content 153 can be decrypted with the second content key.

20 The content 154 is encrypted information generated by encrypting, with use of a third content key, stream data of a highlights video that includes a behind-the-scenes video of a movie "Galaxy Wars: Part 3" that has not yet been released, in addition to the behind-the-scenes videos of the movies "Galaxy Wars: Part 1" and
25 "Galaxy Wars: Part 2". The content 154 can be decrypted with the third content key.

The third content key is generated from the first content key and the second content key.

In this example, the first content key is stored in a storage area in the radio frequency tag 104, and the second content key is stored in a storage area in the radio frequency tag 114.

FIG. 10B shows the structure of the content 151 in a simplified manner.

The content 151 is composed of three sections: a chapter 161, a chapter 162, and a chapter 163.

The chapter 161 is commercial video for encouraging purchase of the package of "Galaxy Wars: Part 1", and is intended by the creator 10 of the content 151 to be viewed by users who have not purchased the package 101.

The chapter 162 is commercial video for encouraging purchase of the package of "Galaxy Wars: Part 2", and is intended by the content creator to be viewed by users who have not purchased the package 15 111.

The chapter 163 is commercial video for advertising a product or the like that is unrelated to "Galaxy Wars: Part 1" and "Galaxy Wars: Part 2", and is intended by the content creator to be viewed by all users, regardless of whether the user has purchased the packages.

20 Each of the chapters 161, 162, and 163 are played by the BD player 122 following playback path information that indicates playback permission and a playback order.

The path playback information is described later.

<Structure>

25 FIG. 11 is a block diagram showing the structure of the content playback system 100 in terms of function.

<Radio frequency tags 104 and 114>

Specifically, each of the radio frequency tags 104 and 114

is a module composed of an IC that has the function of performing radio communication, an antenna, and a small-capacity storage area.

In terms of function, the radio frequency tag 104 is composed of a communication unit 201, an authentication unit 202, and an information storage unit 203, as shown in FIG. 11.

The communication unit 201 performs radio communication with the BD player 122.

The authentication unit 202 performs authentication processing with the BD player 122 via the communication unit 201.

10 In this example, challenge-response authentication is used in the authentication processing.

The following describes challenge-response authentication.

The BD player 122 and the authentication unit 202 store a parent password in advance.

15 The BD player 122 generates a random number, and transmits the random number to the authentication unit 202.

The authentication unit 202 calculates a child password that is a hash value of information that consists of the parent password and the random number, and transmits the child password to the BD 20 player 122.

The BD player 122 calculates a hash value of information that consists of the parent password and the random number, and when the calculated hash value matches the child password transmitted by the authentication unit 202, judges that the result of authentication 25 is legal.

The authentication unit 202 receives the authentication result from the BD player 122.

The information storage unit 203 stores the first content key.

When the result of authentication processing by the authentication unit 202 is legal, the information storage unit 203 transmits the first content key of the BD player 122 via the communication unit 201.

5 The radio frequency tag 114 has the same structure as the radio frequency tag 104, and is composed of a communication unit 211, an authentication unit 212, and an information storage unit 213.

The radio frequency tag 114 stores the second content key in the information storage unit 213.

10 <SD card 121>

Specifically, the SD card 121 is a memory card that includes an IC and a large-capacity storage area.

As shown in FIG. 11, in terms of function, the SD card 121 has a content storage unit 221.

15 The content storage unit 221 stores the contents 151 to 154 as described earlier.

<BD player 122>

The communication units 231 and 233 perform radio communication with the radio frequency tags 104 and 114.

20 The authentication unit 232 performs challenge-response authentication processing with the radio frequency tag 104.

The authentication unit 232 outputs a first authentication result, which is the result of the authentication processing, to the control unit 236, and also transmits the first authentication result to the radio frequency tag 104 via the communication unit 231.

The communication unit 231 receives the first content key stored by the information storage unit 203 via the communication unit 201,

and outputs the first content key to the control unit 236.

The authentication unit 234 performs challenge-response authentication processing with the radio frequency tag 114 via the communication unit 233.

5 The authentication unit 234 outputs a second authentication result, which is the result of the authentication processing, to the control unit 236, and also transmits the second authentication result to the radio frequency tag 114 via the communication unit 233.

10 The communication unit 233 receives the second content key stored by the information storage unit 213 via the communication 211, and outputs the second content key to the control unit 236.

15 The control unit 236 obtains the first and second authentication results from the authentication units 232 and 234, and performs playback control of the content stored in the SD card 121, by instructing the decryption unit 237 and the playback unit 238 in accordance with the combination of the authentication results.

The control unit 236 stores, in advance, a playback path selection table relating to the playback path information.

20 FIGs. 12A and 12B show information relating to playback control, stored by the control unit 236.

FIG. 12A is the playback path selection table stored by the control unit 236.

25 The playback path selection table indicates correspondence between combinations of whether each of the first and second authentication results are legal or illegal, and the playback path information.

Here, the playback path information indicates a playback order

in which the chapters are played.

For example, a playback path 261 indicates that the chapters are played in order of chapter 163, chapter 161, and chapter 162.

When both the obtained first and second authentication results 5 indicate illegal, the control unit 236 selects the playback path 261 based on the playback path selection table.

FIG. 12B shows a playback permission judgment table stored in the control unit 236.

The playback permission judgment table indicates 10 correspondence between combinations of whether each of the first and second authentication results are legal or illegal, and content among content 152 to 154 to be played.

For example, when both the obtained first and second authentication results are legal, the control unit 236, in accordance 15 with the playback permission judgment table, controls so that the content 154 is played.

Furthermore, by storing a correspondence table, the control unit 236 understands that the first content key corresponds to the content 152, that the second content key corresponds to the content 20 153, and that the third content key can be generated from the first and second content keys and corresponds to the content 154.

The control unit 236 receives the first content key stored in the information storage unit 203 via the communication 231, and receives the second content key stored in the information storage 25 unit 213 via the communication unit 233.

The decryption unit 237 obtains the first content key and the second content key from the control unit 236.

The decryption unit 237 generates the third content key from

the first content key and the second content key.

Furthermore, when the content that the control unit 236 has judged will be played is encrypted, the decryption unit 237 decrypts the content with the corresponding one of the first to third content 5 keys.

The playback unit 238 plays content instructed by the control unit 236.

The playback instruction obtaining unit 239 obtains the user instruction from the remote control 123, and outputs the user 10 instruction to the control unit 236.

The timer 240 includes a clock and a counter. A timeout value that is a multiple of 1 second is set by the control unit 236 in the counter.

The timer 240 counts down from the time out value, subtracting 15 "1" every one second.

<Operations>

The following describes operations in content playback processing in the content playback system 100, with reference to FIG. 13.

FIG. 13 is a flowchart showing content playback processing in the content playback system 100.

The user inserts the SD card 121 into the SD slot in the BD player 122 (step S101).

The BD player 122 and the SD card 121 are electrically connected.

The user places the radio frequency tags 104 and 114 such that 25 they are in a range in which radio communication with the BD player 122 is possible.

The control unit 236 sets a value "5" in the timer 240, indicating

a timeout value of five seconds (step S102).

The timer 240 counts down from the set value, subtracting "1" every second.

5 The control unit 236 judges whether the present value in the timer 240 is a value "0" that expresses timeout (step S103).

If the timer 240 indicates timeout, the timer 240 judges the result of the unfinished authentication to be illegal, and notifies the authentication result to the control unit 236 (step S104).

10 The communication units 231 and 233 attempt to communicate with a radio frequency tag with which authentication processing has not been performed (step S105).

If neither of the communication units 231 and 233 is able to communicate with the radio frequency tag with which authentication processing has not been performed, the process returns to step S103.

15 If one of the communication units 231 and 233 are able to communicate with the radio frequency tag with which authentication processing has not been performed, authentication processing is performed (step S106).

20 The authentication processing is challenge-response authentication as described earlier, and the authentication result is either "legal" or "illegal".

The authentication unit that performed authentication notifies the authentication result to the control unit 236 (step S107).

The control unit 236 stores the authentication result.

25 The control unit 236 judges whether all authentication processing has finished by checking whether or not all authentication results that should have been obtained have been obtained (step S108).

If the control unit 236 judges that all authentication

processing has not finished, the processing returns to step S103 and continues.

When the control unit 236 judges that all authentication processing has finished, the processing proceeds to step S109.

5 The control unit 236 instructs the timer 240 to stop the count down, thereby ending timeout measurement processing (step S109).

The control unit 236 selects a playback path corresponding to the combination of obtained authentication results, from the playback path selection table (step S110).

10 The control unit 236 selects encrypted information corresponding to the combination of authentication results, from the playback permission judgment table (step S111).

The decryption unit 237 obtains the first content key and the second content key from the control unit 236, and generates the third 15 content key (step S112).

The decryption unit 237 decrypts the selected encrypted content using the corresponding one of the first to third content keys, and outputs the decrypted content to the playback unit 238.

The playback unit 238 plays the content 151 following the 20 selected playback path (step S113).

The playback unit 238 then plays the next decrypted content received from the decryption unit 237.

<Third Embodiment>

25 The following describes a third embodiment of the present invention with use of the drawings.

<Overview>

FIG. 14 is a schematic drawing of a content playback system

300 of the third embodiment of the present invention.

A BD player 332 is a content playback apparatus that plays content stored on a BD-ROM or an SD card. The BD player 332 includes a function of performing radio communication with a radio frequency 5 tag.

A package 301 is composed of a BD-ROM 302, which is a medium on which content is stored, a box 303 in which the BD-ROM 302 is stored, and a radio frequency tag 304 that is an authentication device attached to the box 303.

10 The radio frequency tag 304 performs radio communication with the BD player 332.

The content recorded on the BD-ROM 302 is stream information that is a data stream of audio and video of the movie called "Galaxy Wars, Part 1."

15 A package 311 is composed of a BD-ROM 312, a box 313 that stores the BD-ROM 312, and a radio frequency tag 314 that is attached to the box 313.

The radio frequency tag 314 performs radio communication with the BD player 332.

20 The BD-ROM 312 stores stream information of a data stream relating to audio and video of the movie of the title "Galaxy Wars: Part 2", which is the sequel to "Galaxy Wars: Part 1" recorded on the BD-ROM 302.

25 A package 321 is composed of a BD-ROM 322, a box 323 that stores the BD-ROM 322, and a radio frequency tag 324 that is attached to the box 323.

The radio frequency tag 324 performs radio communication with the BD player 332.

The BD-ROM 322 stores stream information of a data stream relating to audio and video of the movie of the title "Galaxy Wars: Part 3", which is the sequel to "Galaxy Wars: Part 2".

Here, it is assumed that a user of the BD player 332 already 5 possesses the packages 301, 311 and 321.

In order to have the BD player 332 play the content recorded in either the package 301, 311, or 321, the user inserts the one of the BD-ROMs 302, 312 and 322 that stores the content that the 10 user wishes to play into a predetermined BD-ROM slot of the BD player 332.

The BD player 332 reads and plays content recorded on the inserted BD-ROM.

Furthermore, the user transmits user instructions to the BD player 332 with use of a remote control 333 by pressing operation 15 keys such as a fast forward key, a rewind key, and a stop key.

On receiving a user instruction, the BD player 332 performs control relating to content playback, such as fast forwarding, rewinding, and stopping, according to the user instruction.

The SD card 331 is a recording medium on which content is recorded, 20 and is distributed to the user separately to the package 301, 311 or 321.

The SD card 331 is connected to the BD player 332 by being mounted in a predetermined SD card slot therein.

The SD card 331 stores three contents: content 341, content 25 342, and content 343.

Here, each of the contents 341 to 343 is data stream information that is a data stream of audio and video of a movie.

<Structure>

FIG. 15 is a block diagram showing the structure of the content playback system 300 that is the third embodiment of the present invention.

5 <Radio frequency tag 304, radio frequency tag 314, and radio frequency tag 324>

Specifically, each of the radio frequency tags 304, 314 and 324 is a module composed of an IC that has the function of performing radio communication, an antenna, and a small-capacity storage area.

10 As shown in FIG. 15, in terms of function, the radio frequency tag 304 includes a communication unit 351 and an information storage unit 352.

The communication unit 351 performs radio communication with the BD player 332.

15 The information storage unit 352 stores a medium designation identifier that identifies an SD card whose use is anticipated.

The value of the medium designation identifier stored by the information storage unit 352 is "3".

20 The information storage unit 352 transmits the medium designation identifier to the BD player 332 via the communication unit 351.

The radio frequency tags 314 and 324 have the same structure as the radio frequency tag 304.

The value of the medium designation identifier stored in the information storage unit 362 is "1".

25 The value of the medium designation identifier stored in the information storage unit 372 is "3".

<SD card 331>

The SD card 331 includes a communication unit 381, and

authentication 382, and a content storage unit 383.

SD cards are each assigned a medium identifier for identifying the medium.

In this example, the value of the medium identifier of the
5 SD card 331 is set as "3".

The authentication unit 382 stores the medium identifier.

The communication unit 381 performs communication of information with the BD player 332.

The authentication unit 382 performs authentication processing
10 with the BD player 332 via the communication unit 381.

In this example, challenge-response authentication is used in the authentication processing.

The following describes the challenge and response authentication.

15 The BD player 332 and the authentication unit 382 store a parent password in advance.

The BD player 332 generates a random number, and transmits the random number to the authentication unit 382.

20 The authentication unit 382 calculates a child password that is a hash value of information that consists the parent password and the random number, and transmits the child password to the BD player 332.

25 The BD player 332 calculates a hash value of information that consists of the parent password and the random number, and when the calculated hash value matches the child password transmitted by the authentication unit 382, judges that the result of authentication is legal. Furthermore, when the calculated hash value does not match the child password, the authentication result is illegal.

The authentication unit 382 transmits the medium identifier to the BD player during authentication processing.

The content storage unit 383 stores the content 341, the content 342, and the content 343.

5 The information stored in the content storage unit 383 is read by the BD player 332 via the communication unit 381.

<BD player 332>

10 The communication unit 391 performs radio communication with the radio frequency tag 304, the radio frequency tag 314, and the radio frequency tag 324.

The authentication unit 392 performs challenge-response authentication processing with the authentication 382 via the communication unit 393 and the communication unit 381.

15 The authentication unit 392 outputs the result of the authentication processing to the control unit 394.

The control unit 394 obtains the authentication result from the authentication unit 392.

20 The authentication unit 392 obtains the medium identifier held by the authentication unit 392 from the authentication unit 382 during authentication.

When the authentication result is legal, the control unit 394 plays the content stored on the SD card 331, based on a stored content playback control table.

FIG. 16 shows the content of the content playback control table.

25 The content playback control table indicates correspondence between "match counts" and content that is to be played. Each match count indicates a count of received medium identifiers that match a medium identifier of a medium storing content.

For example, in the present embodiment, since the value of the medium identifier read from the SD card 331 is "3", the value of the medium designation identifier obtained from the radio frequency tag 304 is "3", the value of the medium designation identifier obtained from the radio frequency tag 314 is "1", and the value of the medium designation identifier obtained from the radio frequency tag 334 is "3", the match count is 2.

Consequently, following the content playback control table, the control unit 394 judges that the content 324 is to be played.

The control unit 394 notifies the playback unit 395 of the content to be played back that was selected in accordance with the content playback control table.

The playback unit 395 plays the content 342, which is the content to be played back in accordance with the notification from the control unit 394.

A playback request obtaining unit 396 obtains the user instruction from the remote control 333, and outputs the obtained user instruction to the control unit 394.

The timer 397 includes a clock and a counter. A timeout value that is a multiple of 1 second is set by the control unit 394 in the counter.

The timer 397 counts down from the time out value, subtracting "1" every one second.

<Operations>

The following describes operations in content playback processing in the content playback system 300, with reference to FIG. 17.

FIG. 17 is a flowchart showing content playback processing

in the content playback system 300.

The user inserts the SD card 331 into the SD slot in the BD player 332 (step S201).

The BD player 332 and the SD card 331 are electrically connected.

5 The user places the radio frequency tags 304, 314 and 324 such that they are in a range in which radio communication with the BD player 332 is possible.

The control unit 394 sets a value "5" in the timer 397, indicating five seconds as the timeout value (step S202).

10 The timer 397 counts down from the set value, subtracting "1" every second.

The control unit 394 judges whether the present value in the timer 397 is a value "0" that expresses timeout (step S203).

15 If the timer 397 indicates timeout, the processing proceeds to step S207.

If the timer 397 does not indicate timeout, the BD player 332 attempts to detect a radio frequency tag whose medium designation identifier has not been notified, with the intention of communicating with the detected radio frequency tag (step S204).

20 When such a radio frequency tag is not detected at step S204, the processing returns to step S203.

When such a radio frequency tag is detected at step S204, the BD player 332 obtains the medium designation identifier from the detected radio frequency tag (step S205).

25 The BD player 332 judges whether or not it has communicated with all radio frequency tags with which it was intending to communicate (step S206).

If the BD player 332 judges at step S206 that communication

has not finished, the processing returns to step S203.

If the BD player judges at step S206 that communication has finished, the control unit 394 notifies the timer 397 of the end of timeout detection (step S207).

5 The timer 397 ends timeout detection processing, and clears the counted value.

The control unit 394 selects the content to be played, based on the content playback control table (step S208).

10 The playback unit 395 plays the content selected at step S208
10 (step S209).

<Modifications>

15 The content playback system of the present invention is not limited to the described embodiments. Various modifications may be made in a range that does not deviate from the scope of the present
15 invention.

(1) In the second and third embodiments, a radio frequency tag is used as the medium that performs authentication, and BD-ROMs and SD cards are used as the media which store the content. However, the media are not limited to these, and may be media and/or apparatuses
20 having equivalent functions, such as any of an MO, a DVD, a DVD-ROM, a DVD-RAM, a semiconductor memory, or an IC card, or a mobile telephone or a PDA in which is mounted an LSI having an authentication function.

25 The content playback apparatus that performs authentication is not limited to being a BD player, but may be any apparatus having equivalent functions, such as a DVD player, a personal computer, a video deck, or a home server that includes an HDD.

(2) Although the challenge-response authentication is described as being used in the second and third embodiments, any

authentication method may be used as long as authentication can be performed.

Examples of other authentication methods are one time password authentication, and authentication using a digital signature.

5 Furthermore, examples of secure authentication methods includes a method using PKI, a method using media key obtaining means used in CPRM for DVD-RAM, and a media key obtaining method with mutual authentication used in CPRM for SD.

10 Furthermore, instead of mutual authentication, authentication processing may be performed by one side only.

The following is a possible structure in the second embodiment: the radio frequency tag-side transmits a tag identifier that identifies the radio frequency tag, and the BD player-side stores, in advance, an authentication identifier identifying a radio frequency 15 tag to be authenticated. The result of authentication is legal if the tag identifier and the authentication identifier match.

(3) If the content playback apparatus performs playback control based on authentication processing, it is unnecessary for the content and other information stored on the SD card or the like to be stored 20 in an encrypted state.

(4) In the second embodiment, when the SD card stores one content, the content may be played if the authentication results of both the radio frequency tag 104 and the radio frequency tag 114 are legal.

(5) Although the content 151 is always played in the second 25 embodiment, a structure is possible in which the content 151 is not played.

Furthermore, the playback permission judgment table in the BD player may be used for other control according to the combinations

of a plurality of authentication processing results.

For example, the playback permission table judgment table may store, in correspondence, combinations of authentication processing results, and processing to be executed following user instructions 5 such as rewind, fast forward, and stop.

With such a structure, the instruction that the user is able to give the BD player using the remote control varies according to the combinations of the authentication processing result.

(6) The number of contents selected for playback with respect 10 to each combination of authentication results is not limited to one, but may be two or more contents that are played one after the other.

Furthermore, instead of no content being played when all the authentication results are illegal, other content may be played in this case.

15 (7) Although the correspondence between the match count judged by the BD player and the instructed content is one-to-one in the third embodiment, it is not limited to being so.

For example, the content 343 may be played if the match count 20 is two or greater. Furthermore, the contents 342 and 343 may be played if the match count is two.

(8) The authentication media and the media on which the contents are recorded are not limited to being separate structures.

For example, the authentication processing by the radio frequency tag 114 in the second embodiment may be performed by the 25 SD card 121, and the radio frequency tag 114 omitted.

(9) The present invention is: a content playback apparatus for playing content, based on authentication results, including: an authentication unit operable to perform first device authentication

with a first authentication device, and perform second device authentication with a second authentication device; a determination unit operable to determine a content playback method based on an authentication result combination of the first and second authentications; and a playback unit operable to play content stored in a content storage medium, based on the determined playback method.

Furthermore, the determination unit may further determines that content playback is prohibited, when both the first device authentication and the second device authentication result in failure, and the playback unit may prohibits playback of the content when content playback is determined to be prohibited.

Furthermore, the playback method may include a playback range of a plurality of contents and a playback order of each playback range, and the playback apparatus may play the content based on the determined playback range of the plurality of contents and the playback order of each playback range.

Furthermore, the present invention is a content playback apparatus for playing content based on authentication results, including: an authentication unit operable to perform first authentication based on first information obtained from a first recording medium, and perform second authentication based on second information obtained from a second recording medium; a determination unit operable to determine a playback method based on a combination of authentication results of the first and second authentications; and a playback unit operable to play content stored in a content storage medium, based on the determined playback method.

Furthermore, the content may be an encrypted digital work, the first information may include a first encryption key, and the

second information includes a second encryption key, the content playback apparatus may further include: a decryption unit operable to generate a content key from the first encryption key and the second encryption key, and decrypt the encrypted digital work with use of 5 the content key, and the playback unit may play the decrypted digital work based on the determined playback method.

Furthermore, the present invention is a playback apparatus, including: an obtaining unit operable to obtain first medium designation information from a first recording medium, and obtain 10 medium designation information from a second recording medium; a read unit operable to read at least one piece of medium identification information from at least one content recording medium; a determination unit operable to determine a content playback method based on how many pieces of the recording medium information match 15 the medium designation information; and a playback unit operable to play content stored on the content storage medium, based on the determined content playback method.

Furthermore, the present invention is a playback method for playing content stored on a content storage medium, based on 20 authentication results, including: an authentication step of performing first device authentication with a first authentication device, and performing second device authentication with a second authentication device; a determination step of determining a content playback method based on an authentication result combination of 25 the first and second authentications; and a playback step of playing content stored in a content storage medium, based on the determined playback method.

Furthermore, the present invention is a program applied to

a content playback apparatus for playing content stored on a content storage medium, based on authentication results, the program having executed on a computer: an authentication step of performing first device authentication with a first authentication device, and 5 performing second device authentication with a second authentication device; a determination step of determining a content playback method based on an authentication result combination of the first and second authentications; and a playback step of playing content stored in a content storage medium, based on the determined playback method.

10 Furthermore, the present invention is a content playback system composed of a content playback apparatus for playing content, based on authentication results, first and second authentication devices for performing device authentication with the content playback apparatus, and a recording medium on which content is stored, the 15 content playback apparatus including an authentication unit operable to perform first mutual device authentication with the first authentication device, and perform second mutual device authentication with the second authentication device; a determination unit operable to determine a content playback method based on an 20 authentication result combination of the first and second device authentications; and a playback unit operable to play content stored in the content storage medium, based on the determined playback method.

25 (10) The present invention may be methods shown by the above. Furthermore, the methods may be a computer program realized by a computer, and may be a digital signal of the computer program.

Furthermore, the present invention may be a computer-readable recording medium apparatus such as a flexible disc, a hard disc, a CD-ROM, an MO, a DVD, a DVD-ROM, a DVD RAM, a BD (Blu-Ray Disc),

or a semiconductor memory, that stores the computer program or the digital signal. Furthermore, the present invention may be the computer program or the digital signal recorded on any of the aforementioned recording media.

5 Furthermore, the present invention may be the computer program or the digital signal transmitted on a electric communication line, a wireless or wired communication line, or a network of which the Internet is representative.

10 Furthermore, the present invention may be a computer system that includes a microprocessor and a memory, the memory storing the computer program, and the microprocessor operating according to the computer program.

15 Furthermore, by transferring the program or the digital signal to the recording medium apparatus, or by transferring the program or the digital signal via a network or the like, the program or the digital signal may be executed by another independent computer system.

Industrial Applicability

20 The present invention can be produced by a manufacturer of electronic products such as players for playing digital content stored on a BD-ROM, DVD, SD card or the like, and can be used in a system in which digital content is distributed and played while maintaining protection of copyright of the digital content.

Claims

1. A content playback apparatus for obtaining encrypted content that has been generated by encrypting content with use of a first key, 5 decrypting the obtained encrypted content, and playing the decrypted content,

the content being encrypted based on the first key, the first key being generated by applying a predetermined operation to key generation information based on a second key, the second key being recorded on a recording medium so as to be extractable from the recording 10 medium according to a predetermined procedure,

the content playback apparatus comprising:

a key obtaining unit operable to extract the second key from the recording medium according to the predetermined procedure;

15 an information obtaining unit operable to obtain the encrypted content and the key generation information from an information source other than the recording medium;

a key generation unit operable to apply the predetermined operation to the obtained key generation information, based on the 20 second key, thereby generating a third key; and

a decryption unit operable to decrypt the encrypted content based on the generated third key.

2. The content playback apparatus of Claim 1, wherein
25 the recording medium has recorded thereon key management information that is generated by encrypting the second key based on a fourth key, and

the key obtaining unit includes:

a key storage sub-unit operable to store the fourth key which has been pre-assigned to the content playback apparatus; an information reading sub-unit operable to read the key management information from the recording medium; and
5 a key obtaining sub-unit operable to obtain the second key by decrypting the key management information with use of the fourth key.

3. The content playback apparatus of Claim 1, wherein
10 the recording medium has recorded thereon key management information that is a list of encrypted second keys that have been generated by encrypting the second key respectively with use of a plurality of keys equivalent to the fourth key, and the key obtaining unit includes:

15 a key storage sub-unit operable to store the fourth key that has been pre-assigned to the content playback apparatus; an information obtaining sub-unit operable to obtain the key management information from the recording medium; and a key obtaining sub-unit operable to obtain the second key by decrypting, based on the fourth key, from among the encrypted second keys of the key management information, the encrypted second key that has been encrypted based on the fourth key.
20

25 4. The playback apparatus of Claim 1, wherein the recording medium has recorded thereon key management information that is a list of encrypted second keys that have been generated by encrypting the second key respectively with use of valid

keys, and

the key obtaining unit includes:

a key storage sub-unit operable to store a plurality
of keys;

5 an information obtaining sub-unit operable to obtain
the key management information from the recording medium; and

a key obtaining sub-unit operable to, when one of the
plurality of keys stored in the key-storage sub-unit matches
one of the valid keys, decrypt, from among the encrypted second
10 keys of the key management information, an encrypted second
key that has been encrypted based on the matching key, thereby
obtaining the second key.

5. The content playback apparatus of Claim 1, wherein

15 the recording medium has recorded thereon key management
information including a list of encrypted fifth keys that have been
generated by encrypting a fifth key respectively with a plurality
of keys, and an encrypted second key that has been generated by
encrypting the second key with the fifth key, and

20 the key obtaining unit includes:

a key storage sub-unit operable to store a fourth key
that has been pre-assigned to the content playback apparatus;

an information obtaining sub-unit operable to obtain
the key management information from the recording medium;

25 a first key obtaining sub-unit operable to decrypt the
encrypted fifth keys of the key management information
respectively with use of the fourth key; and

a second key obtaining sub-unit operable to, when the

decryption by the first key obtaining sub-unit succeeds, decrypt the encrypted second key with the fifth key resulting from the decryption by the first key obtaining sub-unit, thereby obtaining the second key.

5

6. The content playback apparatus of Claim 1, wherein the key generation information is an encrypted first key that has been generated by encrypting the first key with use of the second key, and

10 the key generation unit generates the third key by decrypting the obtained key generation information with the second key.

7. The content playback apparatus of Claim 1, wherein the key generation information is arbitrary data of a predetermined length, and is in correspondence with the content, and

the first key has been obtained as a result of subjecting the key generation information to one-way function processing according to a predetermined encryption method, based on the second key, and

20 the key generation unit subjects the key generation information to one-way function processing based on a predetermined encryption method, based on the second key, and treats resultant data as the third key.

25 8. The content playback apparatus of Claim 7, wherein the first key is an exclusive OR of the key generation information and encrypted key generation information generated by encrypting the key generation information based on the predetermined encryption

method, with use of the second key, and
the key generation unit includes:

an encryption sub-unit operable to encrypt the key
generation information based on the predetermined encryption
method, with use of the second key; and

5 a calculation sub-unit operable to calculate an
exclusive OR of the key generation information and the encrypted
key generation information, and treat the resultant data as
the third key.

10

9. The content playback apparatus of Claim 8, wherein
the predetermined encryption method is an AES encryption method,
and

15 the encryption unit encrypts the key generation information
according to the AES encryption method, based on the second key.

10. The content playback apparatus of Claim 1, wherein
the information obtaining unit obtains the encrypted content
and the key generation information via a network.

20

11. The content playback apparatus of Claim 1, wherein
the information obtaining unit obtains the encrypted content
and the key generation information from a dependant recording medium
that is separate from the recording medium.

25

12. The content playback apparatus of Claim 11, wherein
the recording medium has recorded thereon key management
information that includes a list of encrypted fifth keys that have

been generated by encrypting a fifth key respectively with each of a plurality of keys, and encrypted key generation information that has been generated by encrypting the key information with the fifth key, and

5 the information obtaining unit includes:

 a key storage sub-unit operable to store a fourth key that has been pre-assigned to the content playback apparatus;

 an information reading sub-unit operable to read the encrypted content and the key management information from the dependant recording medium;

10 a first key obtaining sub-unit operable to decrypt the encrypted fifth keys of the key management information, based on the fourth key; and

 a second key obtaining sub-unit operable to, when the decryption by the first key obtaining sub-unit succeeds, decrypt the encrypted key generation information with use of the fifth key generated as a result of the decryption by the first key obtaining sub-unit.

20 13. The content playback apparatus of Claim 12, wherein
 the information obtaining unit obtains the encrypted content and the key generation information from a memory card separate from the recording medium.

25 14. The content playback apparatus of Claim 12, wherein
 the information obtaining unit obtains the encrypted content and the key generation information from a disc separate from the recording medium.

15. The content playback apparatus of Claim 1, wherein
the encrypted content has been generated by encrypting the
content with use of a block encryption method, based on the first
5 key, and

the decryption unit decrypts the encrypted content with use
of the block encryption method, based on the first key.

16. The content playback apparatus of Claim 15, wherein
10 the encrypted content has been generated by encrypting the
content with use of a C2 encryption method, based on the first key,
and

the decryption unit decrypts the encrypted content with use
of the C2 encryption method, based on the first key.

15
17. The content playback apparatus of Claim 15, wherein
the encrypted content has been generated by encrypting the
content with use of a DES encryption method, based on the first key,
and

20 the decryption unit decrypts the encrypted content with use
of the DES encryption method, based on the first key.

18. The content playback apparatus of Claim 15, wherein
the encrypted content has been generated by encrypting the
25 content with use of an AES encryption method, based on the first
key, and

the decryption unit decrypts the encrypted content with use
of the AES encryption method, based on the first key.

19. A content playback method used in a content playback apparatus that includes a key obtaining unit, an information obtaining unit, a key generation unit and a decryption unit, and is for obtaining encrypted content that has been generated by encrypting content with a first key, and playing the decrypted content,

the content being encrypted based on the first key, the first key being generated by applying a predetermined operation to key generation information based on a second key, the second key being recorded on a recording medium so as to be extractable from the recording medium according to a predetermined procedure,

the content playback method comprising:
a key obtaining step of extracting the second key from the recording medium according to the predetermined procedure;

an information obtaining step of obtaining the encrypted content and the key generation information from an information source other than the recording medium;

a key generation step of applying the predetermined operation to the obtained key generation information, based on the second key, thereby generating a third key; and

a decryption step of decrypting the encrypted content based on the generated third key.

20. A program applied to a content playback apparatus that includes a key obtaining unit, an information obtaining unit, a key generation unit and a decryption unit, and is for obtaining encrypted content that has been generated by encrypting content with a first key, and playing the decrypted content,

the content being encrypted based on the first key, the first key being generated by applying a predetermined operation to key generation information based on a second key, the second key being recorded on a recording medium so as to be extractable from the recording medium according to a predetermined procedure,

the program having a computer execute:

a key obtaining step of extracting the second key from the recording medium according to the predetermined procedure;

an information obtaining step of obtaining the encrypted content and the key generation information from an information source other than the recording medium;

a key generation step of applying the predetermined operation to the obtained key generation information, based on the second key, thereby generating a third key; and

a decryption step of decrypting the encrypted content based on the generated third key.

FIG. 1

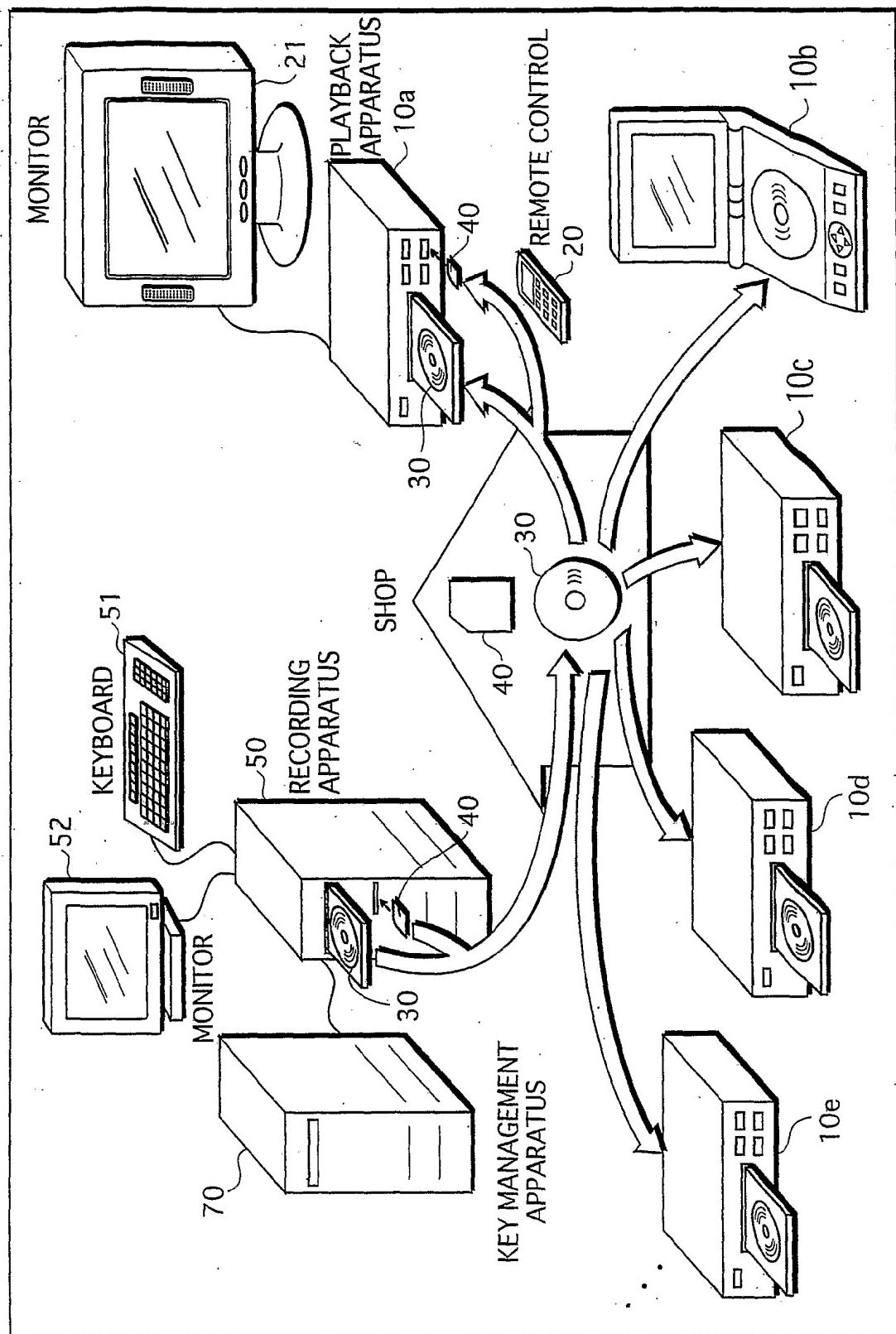


FIG.2

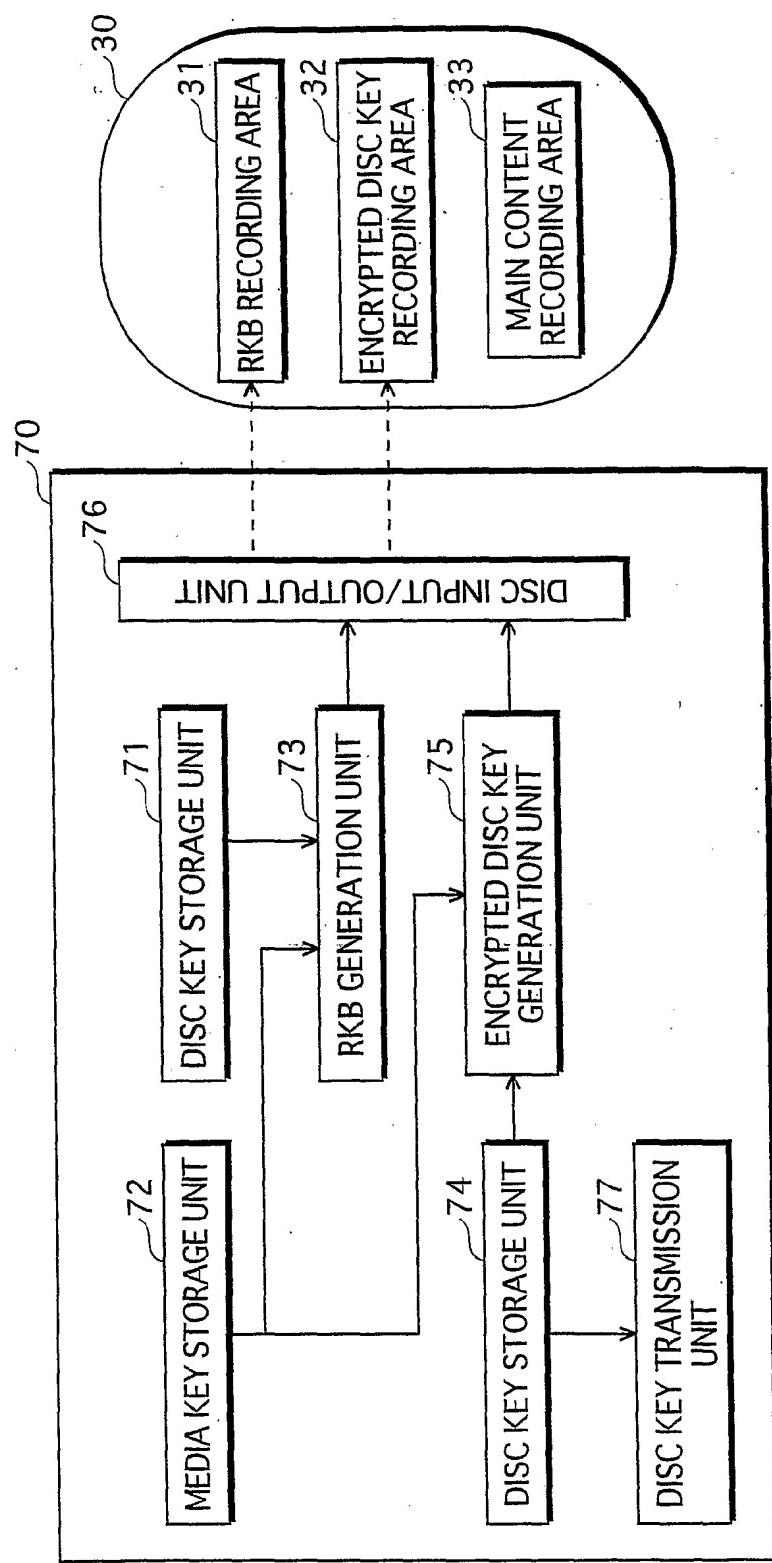
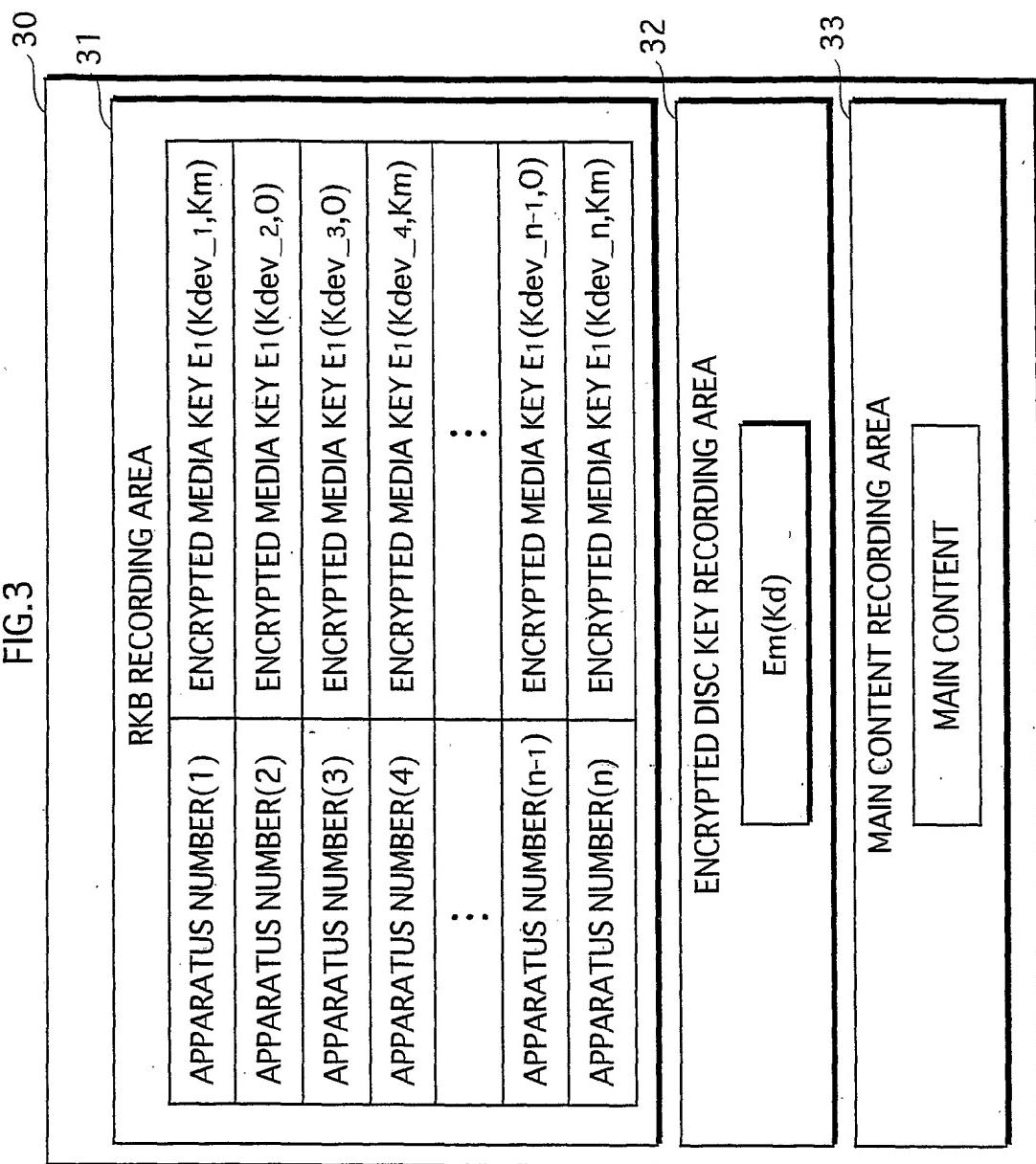


FIG.3



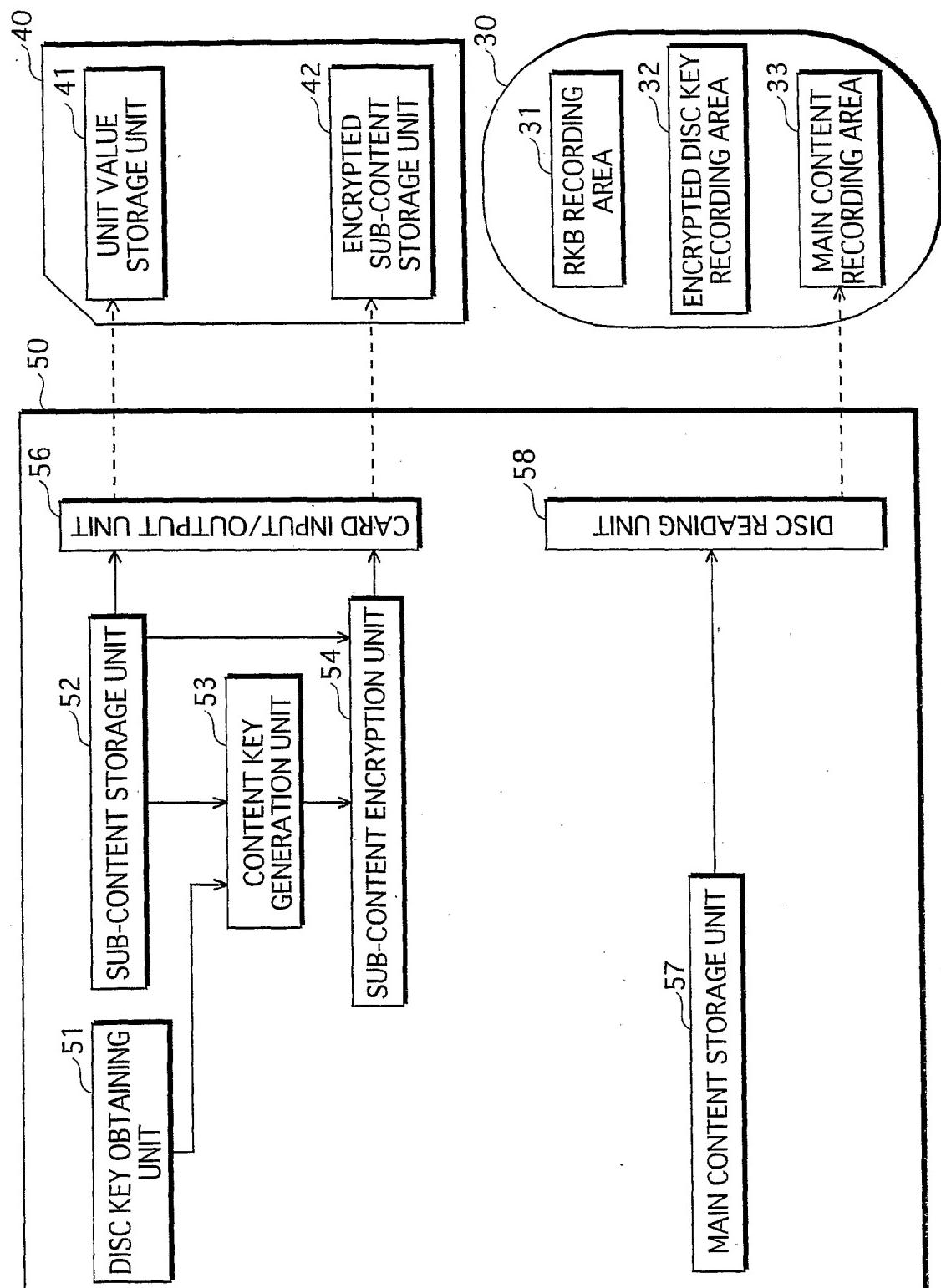


FIG.5

CONTENT NUMBER(1)	UNIT VALUE 1(Vu_1)	SUB-CONTENT 1
CONTENT NUMBER(2)	UNIT VALUE 2(Vu_2)	SUB-CONTENT 2
CONTENT NUMBER(3)	UNIT VALUE 3(Vu_3)	SUB-CONTENT 3
CONTENT NUMBER(4)	UNIT VALUE 4(Vu_4)	SUB-CONTENT 4
:	:	:
CONTENT NUMBER(n-1)	UNIT VALUE n-1(Vu_n-1)	SUB-CONTENT n-1
CONTENT NUMBER(n)	UNIT VALUE n(Vu_n)	SUB-CONTENT n

FIG.6

Vu_1	E2(Kdev_1,SUB-CONTENT 1)
Vu_2	E2(Kdev_2,SUB-CONTENT 2)
Vu_3	E2(Kdev_3,SUB-CONTENT 3)
:	:
Vu_{m-1}	E2(Kdev_{m-1},SUB-CONTENT {m-1})
Vu_m	E2(Kdev_m,SUB-CONTENT m)

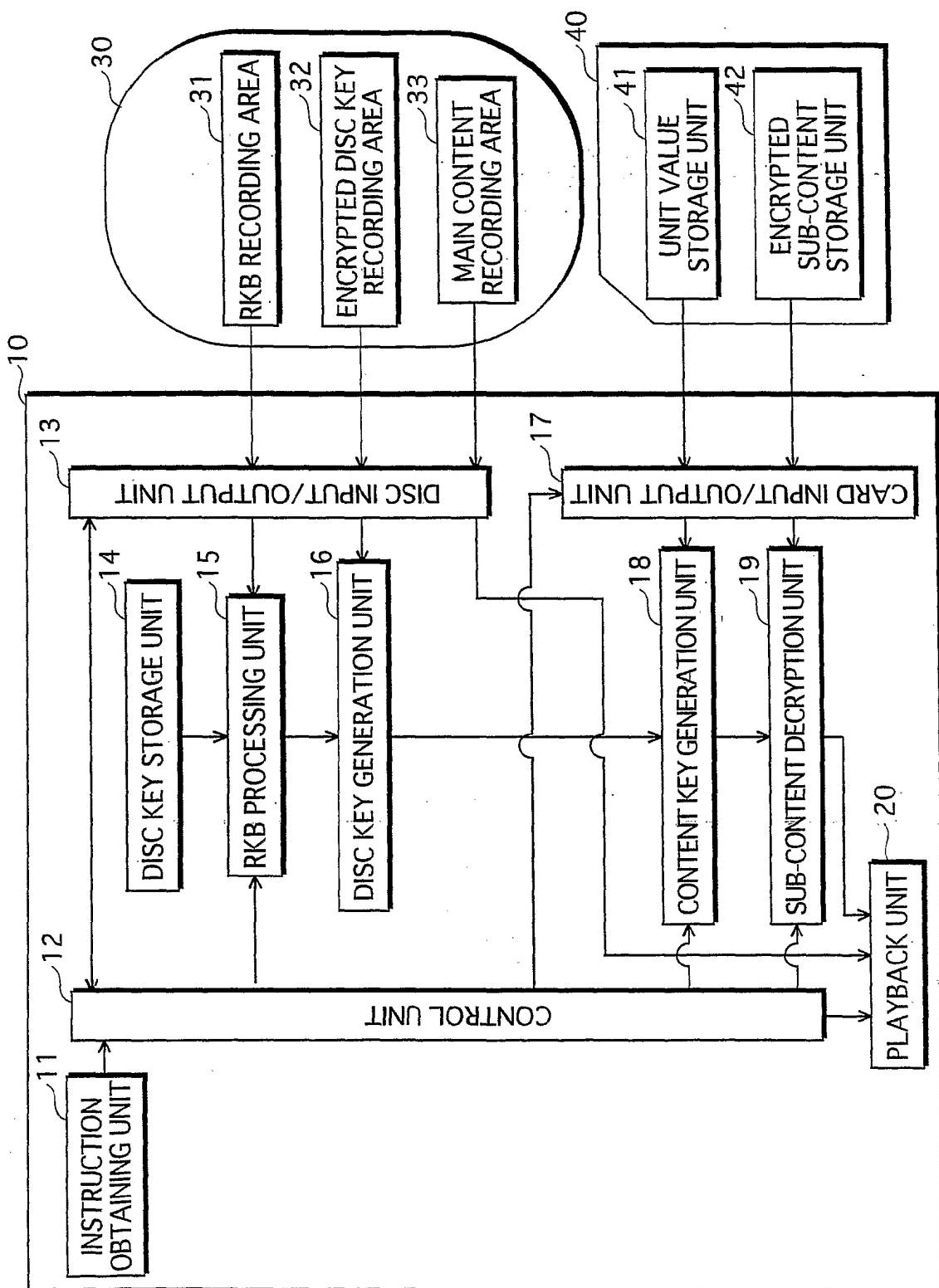


FIG.7

FIG.8

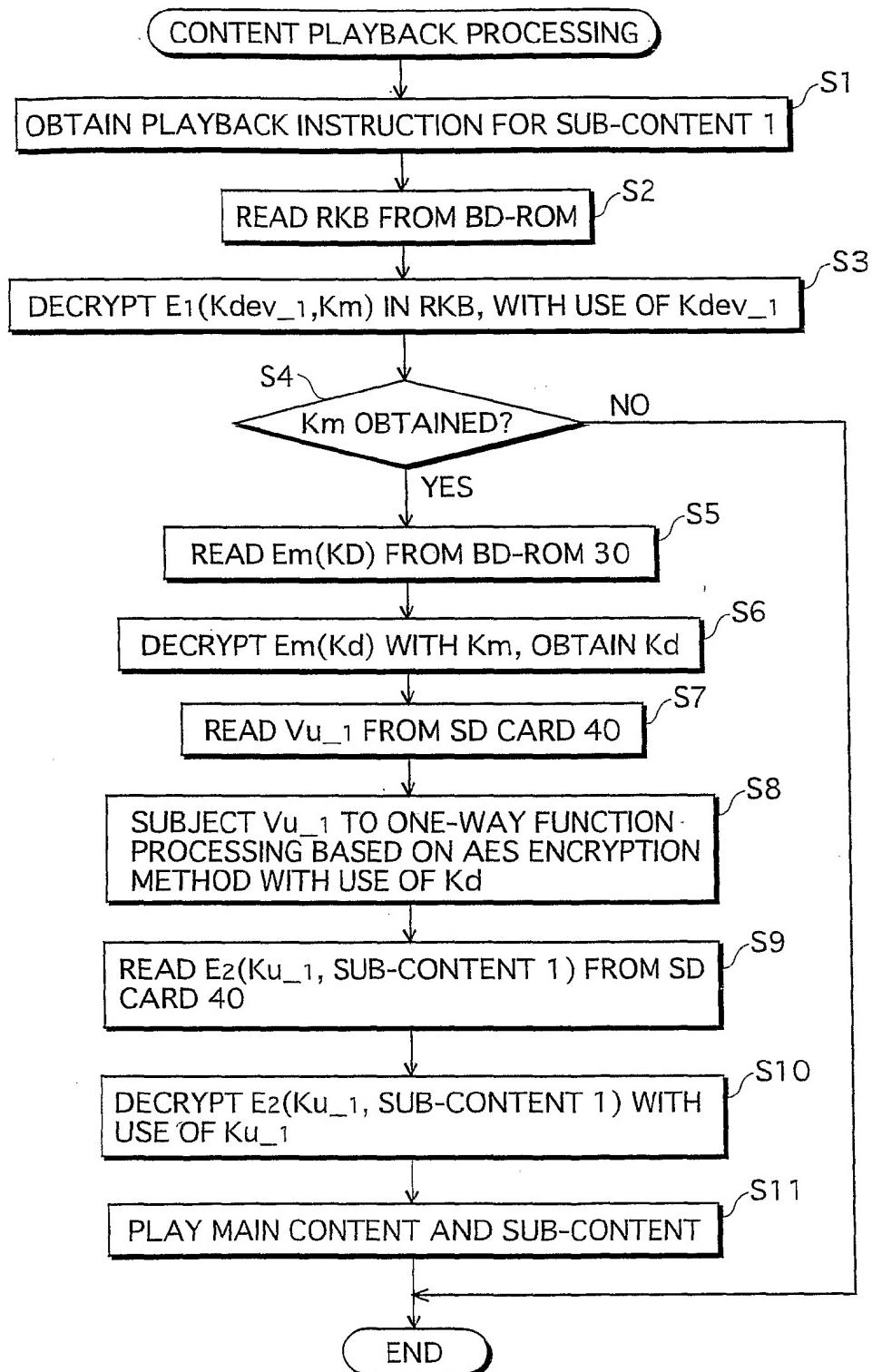


FIG.9

100

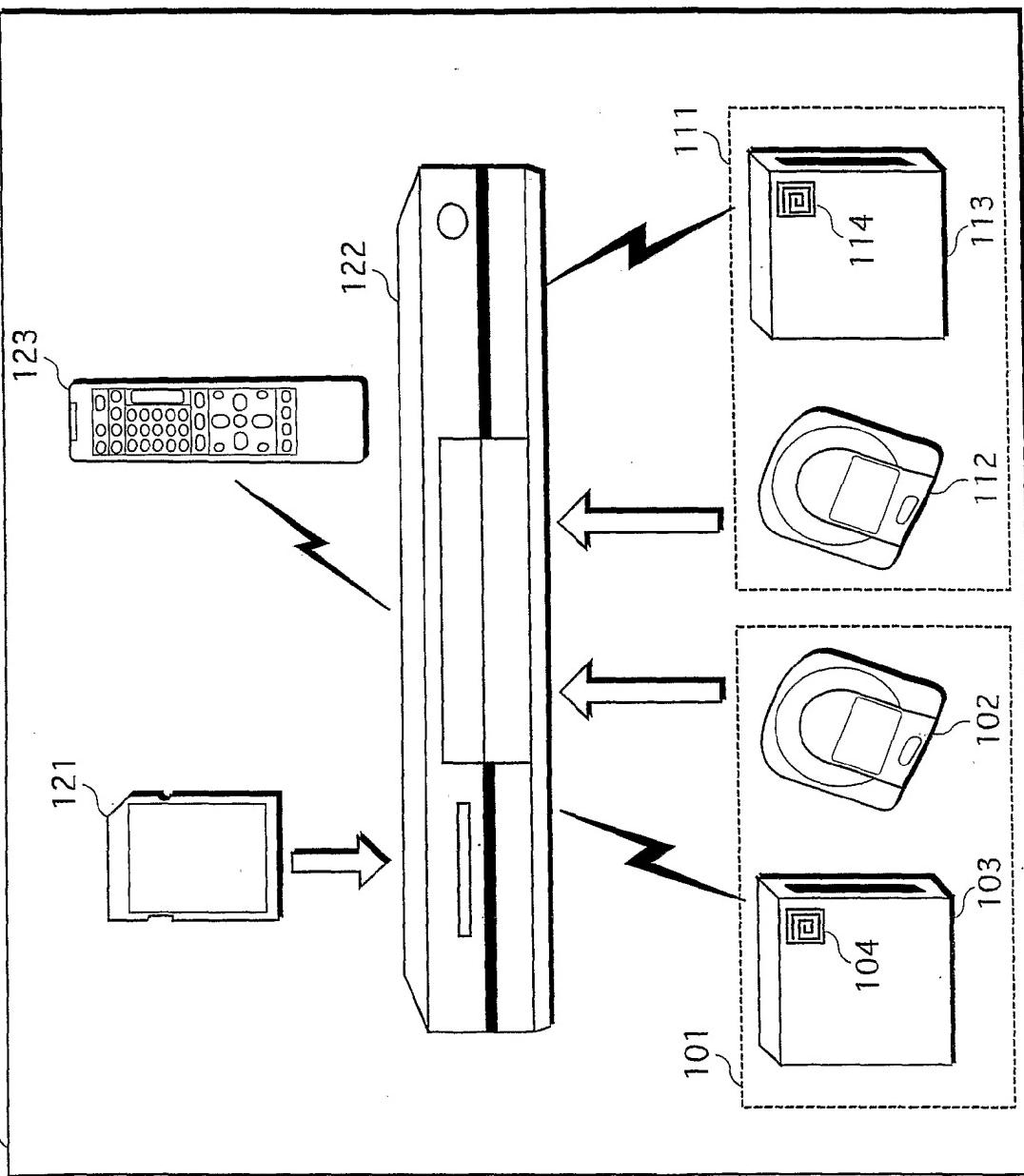


FIG.10A

STORED CONTENT	CORRESPONDING KEY
CONTENT 151	NONE
CONTENT 152	FIRST CONTENT KEY
CONTENT 153	SECOND CONTENT KEY
CONTENT 154	THIRD CONTENT

FIG.10B

CHAPTER 161	CHAPTER 162	CHAPTER 163
-------------	-------------	-------------

FIG.11

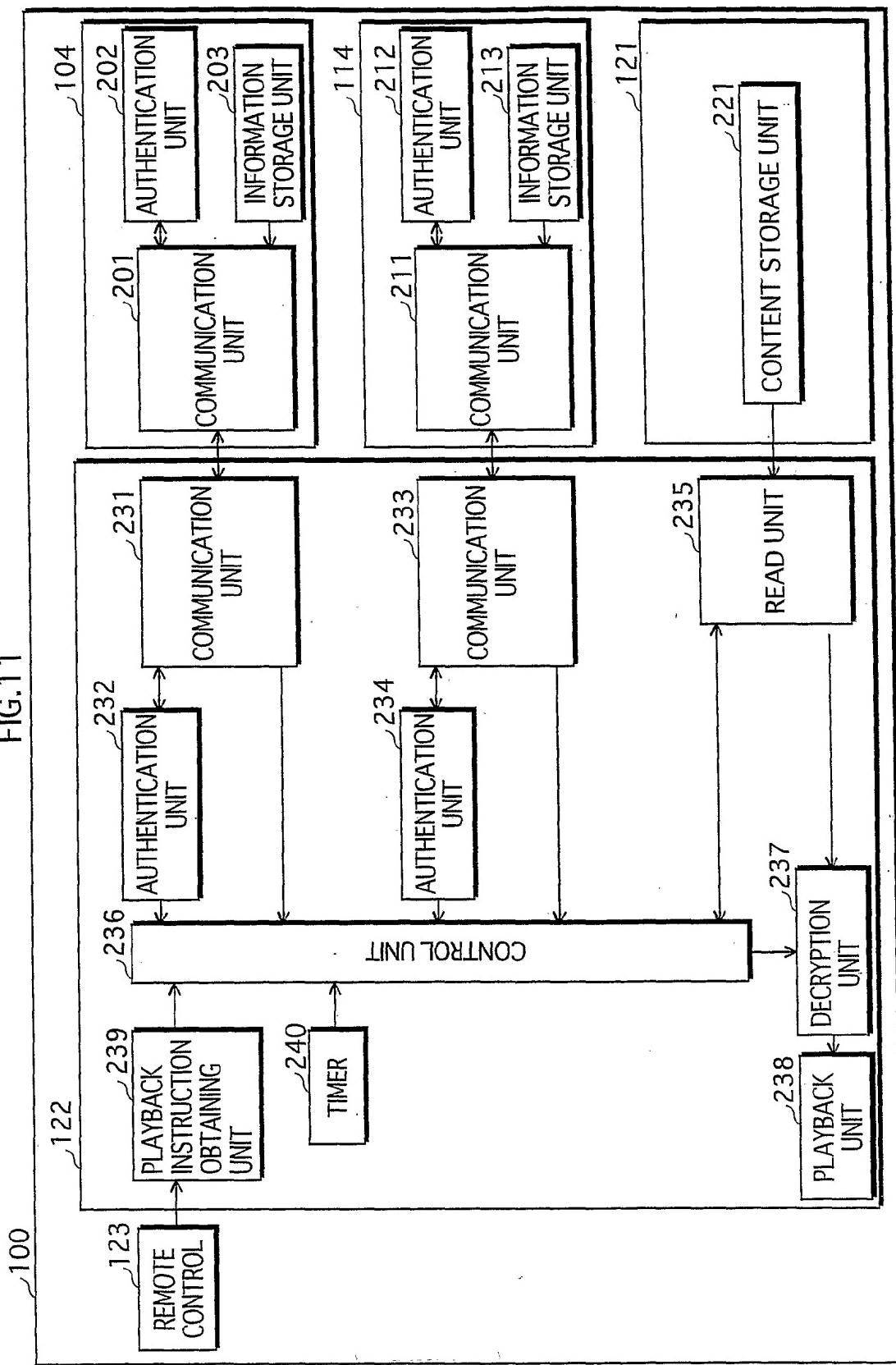


FIG. 12A

FIRST AUTHENTICATION RESULT	SECOND AUTHENTICATION RESULT	PLAYBACK PATH CORRESPONDING OT AUTHENTICATION RESULT COMBINATION
ILLEGAL	ILLEGAL	PLAYBACK PATH 261(CHAPTER 163→CHAPTER 161→CHAPTER 162)
ILLEGAL	LEGAL	PLAYBACK PATH 261(CHAPTER 163→CHAPTER 161)
LEGAL	ILLEGAL	PLAYBACK PATH 261(CHAPTER 163→CHAPTER 162)
LEGAL	LEGAL	PLAYBACK PATH 261(CHAPTER 163)

FIG. 12B

FIRST AUTHENTICATION RESULT	SECOND AUTHENTICATION RESULT	SELECTED CONTENT
ILLEGAL	ILLEGAL	NONE
ILLEGAL	LEGAL	CONTENT 152
LEGAL	ILLEGAL	CONTENT 153
LEGAL	LEGAL	CONTENT 154

FIG.13

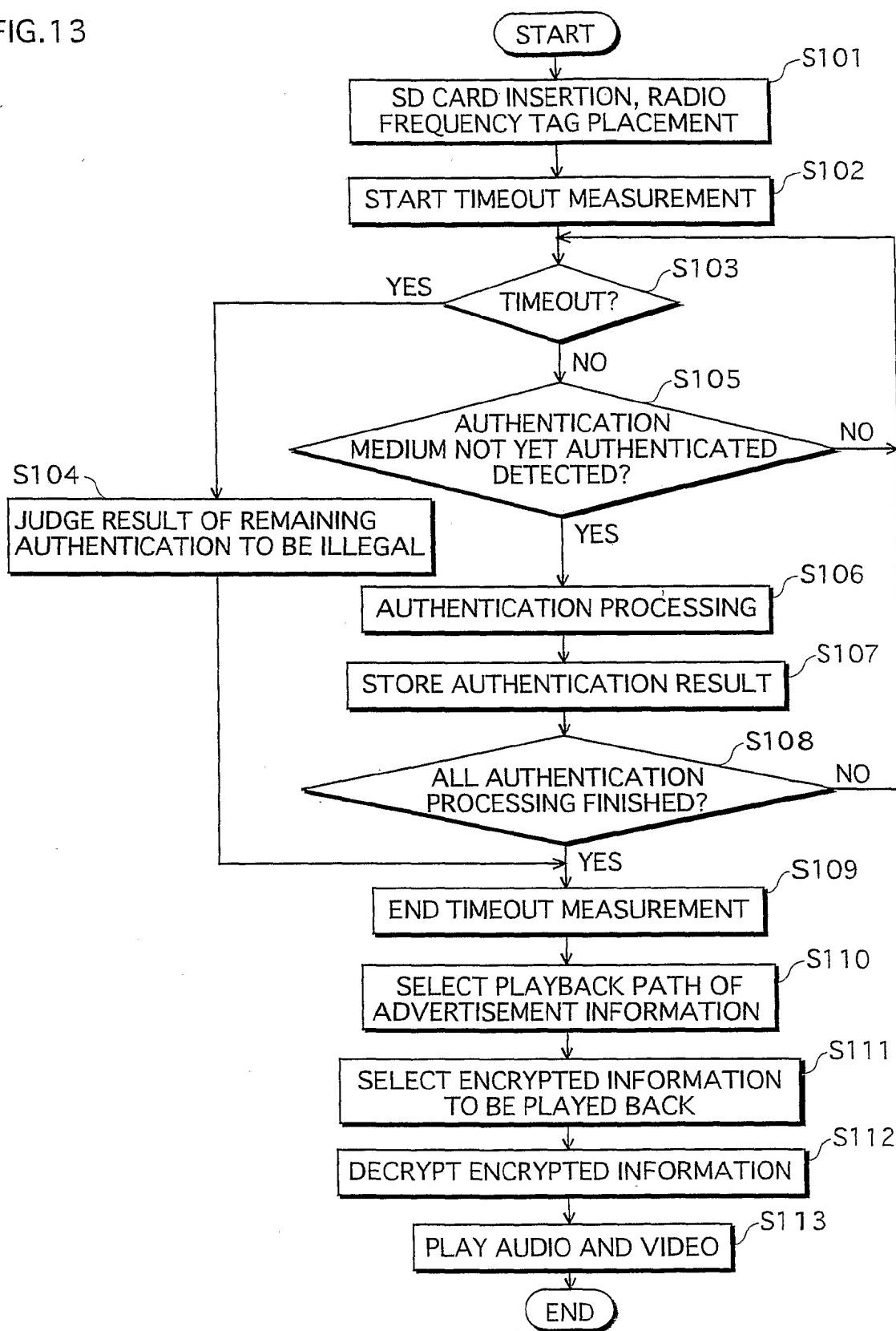


FIG.14

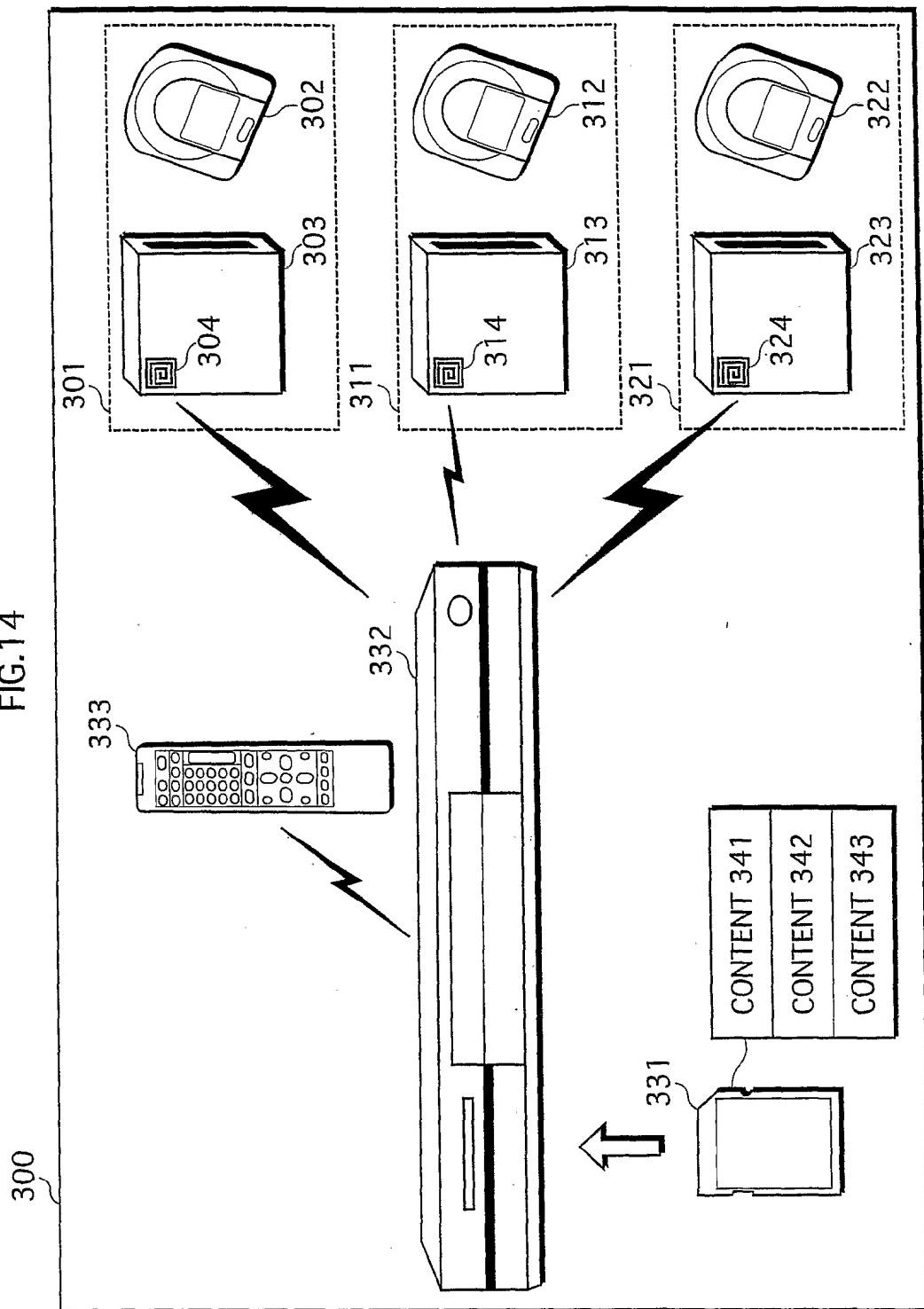


FIG. 15

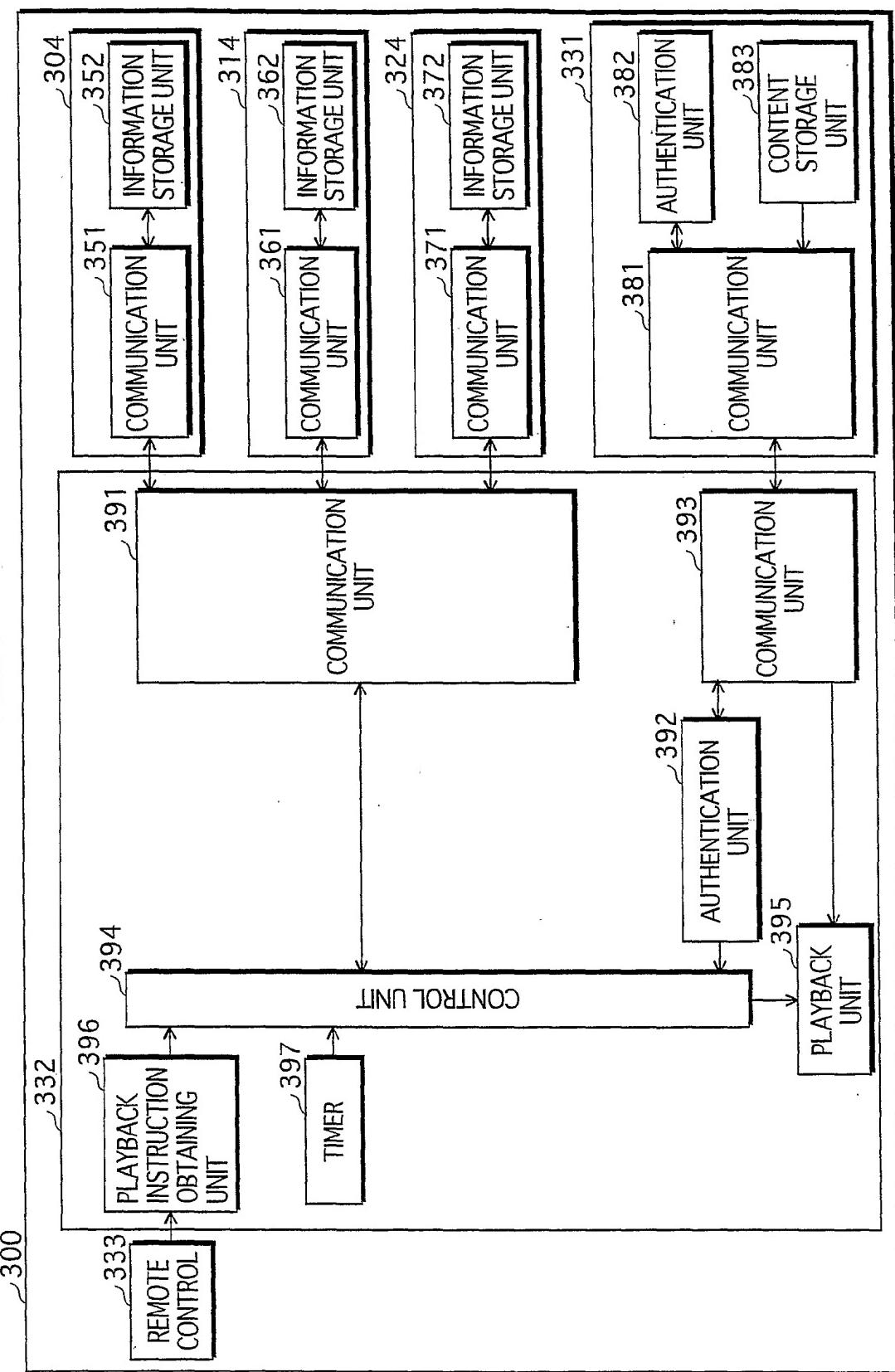
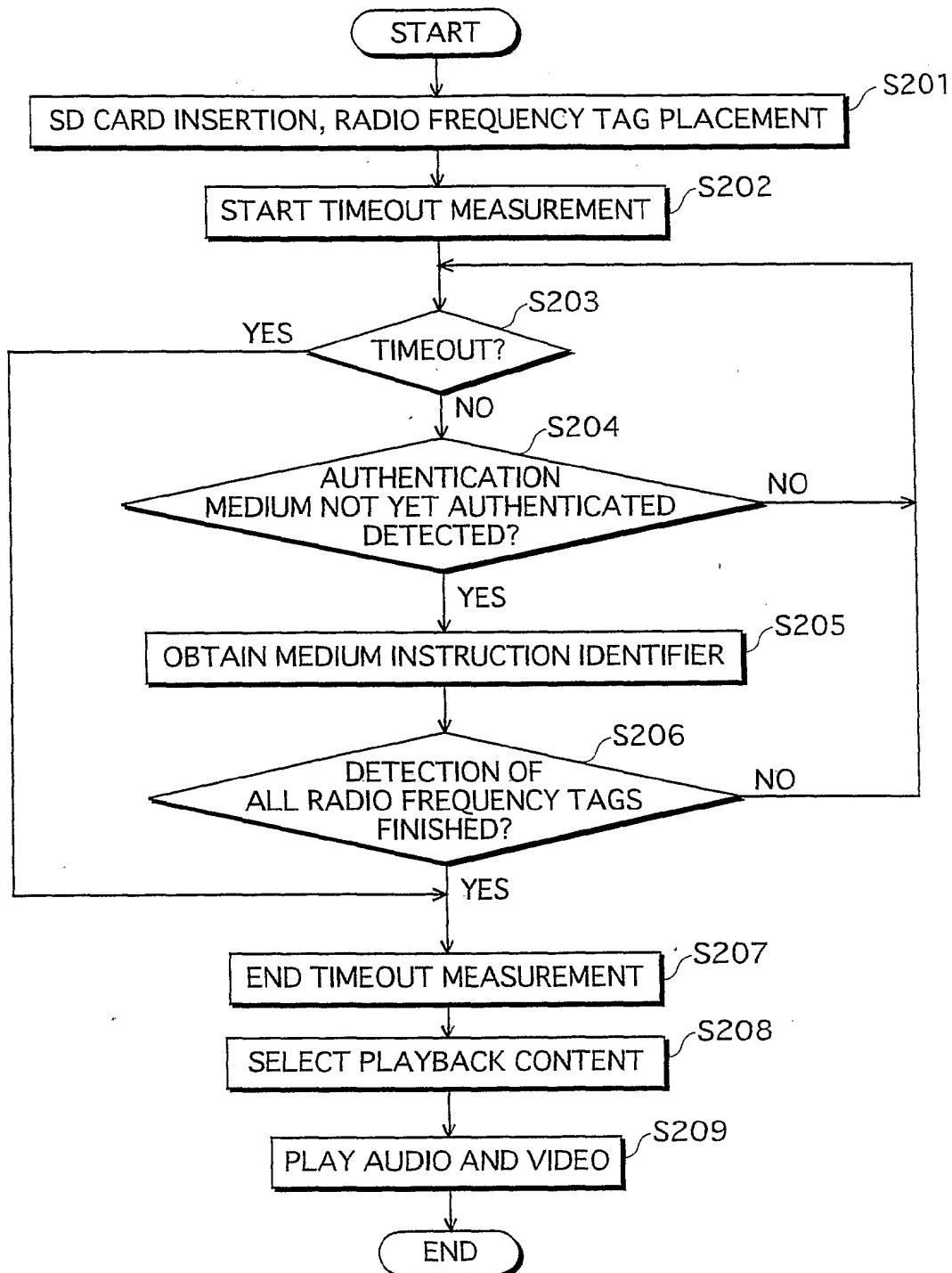


FIG.16

IDENTIFIER MATCH COUNT	SELECTED CONTENT
0	NONE
1	CONTENT 341
2	CONTENT 342
3	CONTENT 343

FIG.17



INTERNATIONAL SEARCH REPORT

Inte al Application No
PCT/JP2004/008554

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96/11446 A (PHILIPS ELECTRONICS NV ; PHILIPS NORDEN AB (SE)) 18 April 1996 (1996-04-18) the whole document	1,7,10, 17,19,20
Y	----- EP 1 185 022 A (SONY CORP) 6 March 2002 (2002-03-06) column 1, line 5 - column 15, line 2 column 34, line 2 - column 36, line 12 column 39, line 53 - column 42, line 57 figures 11-17,19-31,33-39,44-46C	2-6,8,9, 11-15,18
Y	----- EP 1 271 839 A (FUJITSU LTD) 2 January 2003 (2003-01-02) the whole document	2-6,8,12
	----- -----	9,18
	-----	-/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

15 October 2004

29/10/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Barel-Faucheux, C

INTERNATIONAL SEARCH REPORT

Int'l Application No
PCT/JP2004/008554

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DAEMEN J ET AL: "AES PROPOSAL: RIJNDAEL" AES PROPOSAL, XX, XX, 3 September 1999 (1999-09-03), pages 1-45, XP001060386 cited in the application the whole document	9,18
Y	WO 02/095747 A (MICHTCHENKO VALENTIN ALEXANDRO) 28 November 2002 (2002-11-28) the whole document	11,13,14
Y	WO 01/56221 A (VDG INC) 2 August 2001 (2001-08-02) the whole document	15
A	EP 1 185 023 A ('SONY CORP) 6 March 2002 (2002-03-06) column 40, line 20 - column 41, line 36 column 42, line 15 - column 44, line 11 figures 1,2,4,5,7-15,17-19,23,26-28,32-39	1-20
P,X	US 2004/109569 A1 (ELLISON CARL M ET AL) 10 June 2004 (2004-06-10) the whole document	1-20
A	WO 03/032300 A (DOMJAN LASZLO ; ERDEI GABOR (HU); KOPPA PAL (HU); SZARVAS GABOR (HU);) 17 April 2003 (2003-04-17) the whole document	1-20
A	EP 1 215 844 A (MATSUSHITA ELECTRIC IND CO LTD) 19 June 2002 (2002-06-19) cited in the application the whole document	1-20
A	WO 00/51119 A (FAUSSE ARNAUD ; SCHLUMBERGER SYSTEMS & SERVICE (FR)) 31 August 2000 (2000-08-31) the whole document	1-20
A	US 2002/012430 A1 (LIM YOUNG-WON) 31 January 2002 (2002-01-31) the whole document	17

INTERNATIONAL SEARCH REPORT
Information on patent family members

Inte
al Application No
PCT/JP2004/008554

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO 9611446	A	18-04-1996	DE	69531447 D1		11-09-2003
			DE	69531447 T2		01-07-2004
			EP	0733239 A1		25-09-1996
			WO	9611446 A2		18-04-1996
			JP	9507598 T		29-07-1997
			US	5787170 A		28-07-1998
EP 1185022	A	06-03-2002	JP	2001352322 A		21-12-2001
			AU	4684501 A		23-10-2001
			CA	2372545 A1		18-10-2001
			EP	1185022 A1		06-03-2002
			AU	4685701 A		23-10-2001
			CA	2372552 A1		18-10-2001
			CN	1383643 T		04-12-2002
			CN	1383645 T		04-12-2002
			EP	1185023 A1		06-03-2002
			HU	0202148 A2		28-10-2002
			WO	0178300 A1		18-10-2001
			WO	0178301 A1		18-10-2001
			JP	2002063763 A		28-02-2002
			US	2003016826 A1		23-01-2003
			US	2003016827 A1		23-01-2003
EP 1271839	A	02-01-2003	JP	2003015522 A		17-01-2003
			EP	1271839 A2		02-01-2003
			US	2003108195 A1		12-06-2003
WO 02095747	A	28-11-2002	WO	02095747 A1		28-11-2002
			EP	1440438 A1		28-07-2004
			US	2004136536 A1		15-07-2004
WO 0156221	A	02-08-2001	AU	6097001 A		07-08-2001
			EP	1252738 A2		30-10-2002
			WO	0156221 A2		02-08-2001
			US	2001033656 A1		25-10-2001
EP 1185023	A	06-03-2002	JP	2002063763 A		28-02-2002
			AU	4685701 A		23-10-2001
			CA	2372552 A1		18-10-2001
			EP	1185023 A1		06-03-2002
			AU	4684501 A		23-10-2001
			CA	2372545 A1		18-10-2001
			CN	1383643 T		04-12-2002
			CN	1383645 T		04-12-2002
			EP	1185022 A1		06-03-2002
			HU	0202148 A2		28-10-2002
			WO	0178300 A1		18-10-2001
			WO	0178301 A1		18-10-2001
			JP	2001352322 A		21-12-2001
			US	2003016826 A1		23-01-2003
			US	2003016827 A1		23-01-2003
US 2004109569	A1	10-06-2004	WO	2004053867 A2		24-06-2004
WO 03032300	A	17-04-2003	EP	1440434 A2		28-07-2004
			WO	03032300 A2		17-04-2003
EP 1215844	A	19-06-2002	EP	1215844 A2		19-06-2002

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No

PCT/JP2004/008554

Patent document cited in search report	Publication date		Patent family member(s)	Publication date
EP 1215844	A		JP 2002281013 A US 2002076204 A1	27-09-2002 20-06-2002
WO 0051119	A	31-08-2000	FR 2790346 A1 CN 1341259 T EP 1155410 A1 WO 0051119 A1 JP 2002538566 A	01-09-2000 20-03-2002 21-11-2001 31-08-2000 12-11-2002
US 2002012430	A1	31-01-2002	KR 2001012741 A GB 2367461 A ,B JP 2002032018 A TW 514846 B	21-12-2001 03-04-2002 31-01-2002 21-12-2002